Naval Research Laboratory
Washington, DC 20375-5320

NRL/MR/5515--97-8119

Information Technology Division Technical Paper Abstracts 1996

COMPILED BY
MARYALLS G. BEDFORD, M.S.

Sabre Systems, Inc.
Warminster, Pennsylvania

GRAPHIC DESIGNS BY
NINA D'SOUZA

George Washington University

Navy Center for Applied Research in Artificial Intelligence
Information Technology Division

December 15, 1997

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (*Leave Blank*)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 15, 1997	

4. TITLE AND SUBTITLE

Information Technology Division Technical Paper Abstracts 1996

5. FUNDING NUMBERS

6. AUTHOR(S)

Maryalls G. Bedford* and Nina S. D'Souza†

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval Research Laboratory
Washington, DC 20375-5320

8. PERFORMING ORGANIZATION REPORT NUMBER

NRL/MR/5515--97-8119

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Office of Naval Research
Arlington, VA 22217-5660

Sabre Systems, Inc.
Warminster, PA

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

*Sabre Systems, Inc., Warminster, PA
George Washington University

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (*Maximum 200 words*)

This report provides abstracts for technical publications produced during 1996 by personnel of the Information Technology Division (ITD), one of the largest research and development collectives at the Naval Research Laboratory. The abstracts are organized into sections that represent the six branches with ITD: the Navy Center for Applied Research in Artificial Intelligence, Communication Systems, the Center for High Assurance Computer Systems, Transmission Technology, Advanced Information Technology, and the Center for Computational Science. Within each section, a list of branch papers published in 1994 and 1995 has also been included: abstracts for these papers may be found in prior-year editions of this report. Information on obtaining a copy of one or more of the abstracted or listed publications is provided as well.

14. SUBJECT TERMS

15. NUMBER OF PAGES

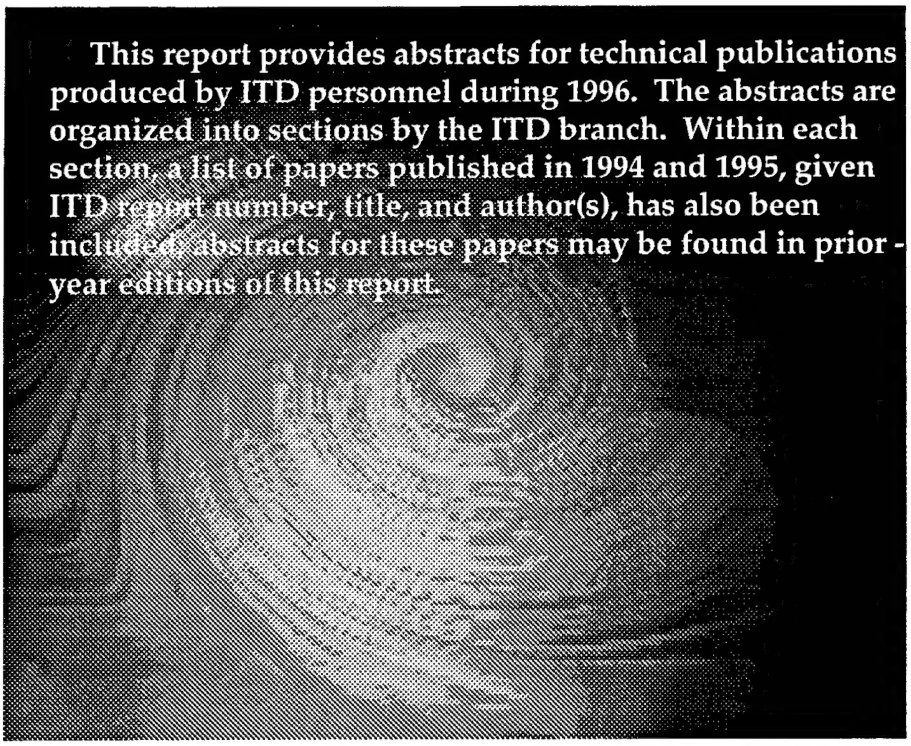
111

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std 239-18
298-102



To obtain a copy of one or more of the abstracted or listed papers, contact the NCARAI librarian at 202-767-0018 (telephone); 202-767-3172 (fax); library@aic.nrl.navy.mil (email); or by postal mail at

Naval Research Laboratory
Attn: NCARAI Library Code 5510
Washington, DC 20375-5337

Please give the report number, title, and author(s) of each paper desired. Additionally, the list of abstracts and a number of the papers (primarily those produced by NCARAI) are available through the WWW at URL: http://www.aic.nrl.navy.mil/papers, or by anonymous FTP to host ftp.aic.nrl.navy.mil (132.250.84.25), in the /pub/papers directory.

Contents . . .

introduction

The Naval Research Laboratory (NRL) is the corporate laboratory for the United States Navy, and employs more than 3,700 civilians to conduct research and development programs in a wide range of technical disciplines. While more than 750 of NRL's employees hold doctorates, all members of the research staff participate extensively in national and international technical groups. In order to inform the research, academic, and industrial communities of its research activities, NRL annually publishes in excess of 1,000 journal articles, technical papers, and reports.

The Information Technology Division (ITD) is one of the largest research and development collectives at NRL. ITD employs more than 220 civilian researchers organized into six branches: the Navy Center for Applied Research in Artificial Intelligence, Communication Systems, the Center for High Assurance Computer Systems, Transmission Technology, Advanced Information Technology, and the Center for Computational Science. The technical areas of expertise in ITD include:

Communications

network simulation
HF communications
communication security
communications networking

Human-Computer Interaction

visualization techniques
metrics and evaluation
speech communication systems
human-computer dialogue

Artificial Intelligence

intelligent simulation
adaptive control software
machine learning methods
robotic vision and control
interactive systems
intelligent decision aids
reasoning under uncertainty

Software

computer security
network security
software assurance
software specification methods
hard real time computing
adaptive software testing
information security

&

Decision Support Systems

parallel processing techniques
distributed decision support
prototyping techniques
distributed simulation

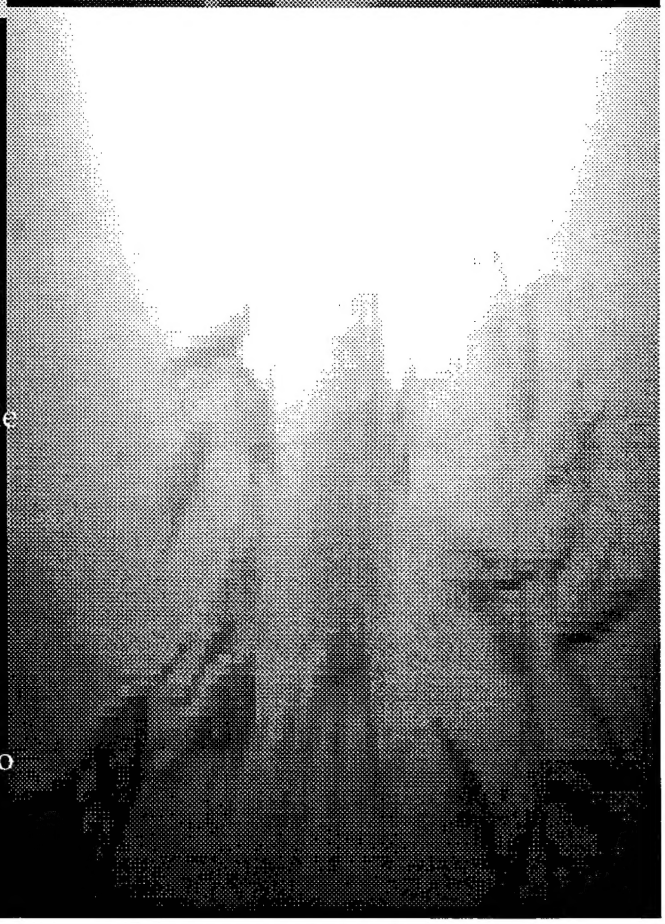
Abstracts Publication 1996

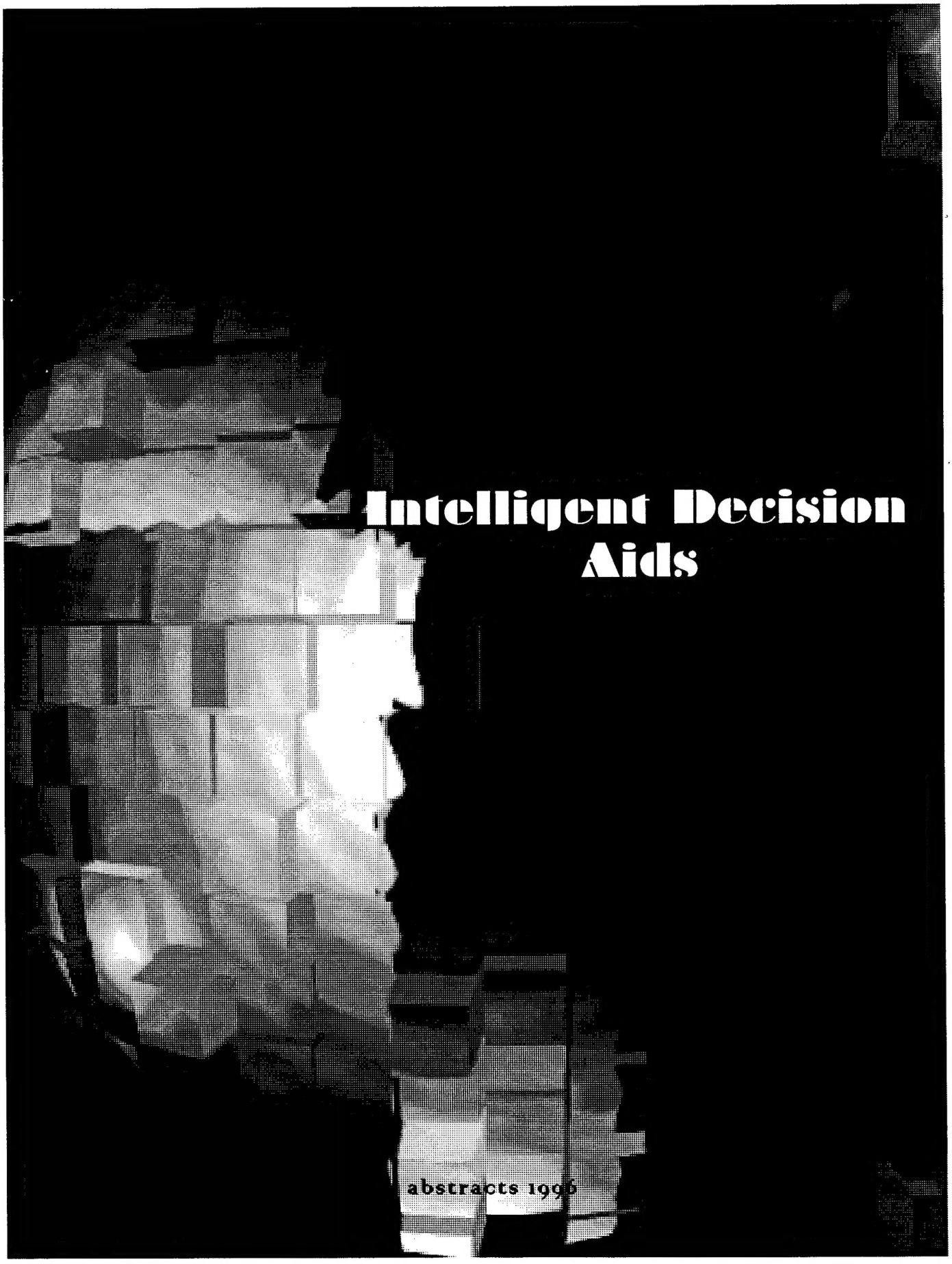
The Navy Center For Applied Research in Artificial Intelligence (NCARAI) is engaged in research efforts designed to address the application of artificial intelligence (AI) technology and techniques critical to Navy and national concerns. The emphasis at NCARAI is the linkage of theory and application in demonstration projects that use a full spectrum of AI methods.

Navy Center For Applied Research In Artificial Intelligence

Code 5510

The technical papers and reports generated by the NCARAI document the accomplishments of projects in computational reasoning for intelligent decision aids, intelligent M4 (multi-media, multi-modal) systems, interface design and evaluation, machine learning, and sensor-based systems. Innovative basic and exploratory research in these areas are made possible by NCARAI's staff, an impressive cross section of AI talent from the Government civilian and military sectors, visiting scholars from the academic communities, and consulting scientists from various industries. An ongoing seminar series, featuring notable scientists and scholars from around the country and from abroad, provides an excellent forum to exchange information and maintain awareness of current developments.




Intelligent Decision Aids
abstracts 1996

INTELLIGENT DECISION AIDS

Title: Greedy Utile Suffix Memory for Reinforcement Learning with Perceptually-Aliased States
Author(s): Leonard A. Breslow
E-mail Address: breslow@aic.nrl.navy.mil
Citation: Internal Report
Date: January 1996
Report No.: AIC-96-004

Abstract

Reinforcement learning agents are faced with the problem of perceptual aliasing when two or more states are perceptually identical but require different actions. Purely reactive policies do not produce optimal performance in such situations. To address this problem, various researchers have incorporated memory of preceding events into the definition of states to distinguish perceptually-aliased states. Approaches to differentiating aliased states engage in two concurrent interacting learning processes: learning of the correct *state representation* and reinforcement learning of the correct *policy* of actions to take from each state. Recently, McCallum (1995b) has offered Utile Suffix Memory (USM), an instance-based algorithm using a tree to store instances and to represent states for reinforcement learning. USM's use of online instance-based state learning permits state definitions to be updated quickly based on the latest results of reinforcement learning. USM uses statistical tests to determine the relevance of history information considered for inclusion in state definitions. However, USM conducts many unnecessary statistical comparisons, making it vulnerable to false positive errors that produce state distinctions that are not useful and over branching of the state tree. The algorithm cannot correct such errors since it does not prune the state tree. The problem of over-branching of the state tree is particularly serious when the algorithm is applied to tasks in which some aliased states cannot be differentiated on the basis of the event immediately prior to the current observation (i.e., at time t-1) but can only be differentiated on the basis of earlier events (e.g., t-2 or t-3). Greedy Utile Suffix Memory (GUSM) addresses these concerns through several modifications of USM: greedy state splitting, incremental state splitting, and the restriction of statistical comparisons to potentially useful differences. GUSM is shown to learn action policies faster than USM and to generate smaller state spaces (i.e., more correctly-sized trees).

Title: Cooperative Bayesian and Case-Based Reasoning for Solving Multiagent Planning Tasks
Author(s): David A. Aha and Liwu W. Chang
E-mail Address: aha@aic.nrl.navy.mil or liwu@aic.nrl.navy.mil
Citation: Internal Report
Date: January 25, 1996
Report No.: AIC-96-005

Manuscript approved August 28, 1997

Abstract

We describe an integrated problem solving architecture named INBANCA in which Bayesian networks and case-based reasoning (CBR) work cooperatively on multiagent planning tasks. This includes two-team dynamic tasks, and this paper concentrates on simulated soccer as an example. Bayesian networks are used to characterize action selection, whereas a case-based approach is used to determine how to implement actions. This paper has two contributions. First, we survey integrations of case-based and Bayesian approaches from the perspective of a popular CBR task decomposition framework, thus explaining what types of integrations have been attempted. This allows us to explain the unique aspects of our proposed integration. Second, we demonstrate how Bayesian nets can be used to provide environmental context, and thus feature selection information, for the case-based reasoner.

Title: Simplifying Decision Trees: A Survey
Author(s): Leonard A. Breslow and David W. Aha
E-mail Address: breslow@aic.nrl.navy.mil or aha@aic.nrl.navy.mil
Citation: Knowledge Engineering Review, v12, n1, 1997, pp1-40
Date: 1996
Report No.: AIC-96-014

Abstract

Induced decision trees are an extensively-researched solution to classification tasks. For many practical tasks, the trees produced by tree-generation algorithms are not comprehensible to users due to their size and complexity. Although many tree induction algorithms have been shown to produce simpler, more comprehensible trees (or data structures derived from trees) with good classification accuracy, tree simplification has usually been of secondary concern relative to accuracy and no attempt has been made to survey the literature from the perspective of simplification. We present a framework that organizes the approaches to tree simplification and summarize and critique the approaches within this framework. The purpose of this survey is to provide researchers and practitioners with a concise overview of tree-simplification approaches and insight into their relative capabilities. In our final discussion, we briefly describe some empirical findings and discuss the application of tree induction algorithms for case retrieval in case-based reasoning systems.

Title: Comparing Tree-Simplification Procedures
Author(s): Leonard A. Breslow and David W. Aha
E-mail Address: breslow@aic.nrl.navy.mil or aha@aic.nrl.navy.mil
Citation: Proceedings of the Sixth International Conference on Artificial Intelligence and Statistics (pp67-74), Ft. Lauderdale, FL: Unpublished
Date: 1996
Report No.: AIC-96-015

Abstract

Decision trees are used in several expert classification systems and are often relied on to comprehensibly summarize data. However, they are often unintelligible and require simplification. Several alternatives have been proposed

to simplify decision trees, but their relative capabilities are largely unknown; their evaluation is usually limited to comparisons with "bench-mark" systems (i.e., C4.5, CART). This paper presents a categorization framework for tree-simplification methods and focuses on their comprehensive empirical comparison.

Title: A WWW Demonstration of Stratified Case-Based Reasoning
Author(s): Jeffrey W. Adams and David W. Aha
E-mail Address: aha@aic.nrl.navy.mil
Citation: Internal Report
Date: July 18, 1996
Report No.: AIC-96-016

Abstract

This paper summarizes the first author's internship (June 24 until July 18, 1996) at the Navy Center for Applied Research in Artificial Intelligence (NCARAI) of the Naval Research Laboratory. The goal for this internship was to create a project that is professional and useful to NCARAI, to explore the capabilities of the World Wide Web (WWW), and to bring that knowledge back to the Naval Academy for his senior year. With this in mind, we focused on developing a WWW demonstration for the artificial intelligence programs described in (Branting & Aha, 1995). They introduced several case-based reasoning (CBR) algorithms that learn by storing solutions to previously solved problems. These solutions were grouped with problem descriptions into cases, which can be reused to decrease the time required to solve similar problems. We researched literature on porting applications to the WWW, organized WWW information related to this topic in a WWW page, and helped to develop a WWW interface for these CBR algorithms.

Title: Adjustable Graphic-Based Clustering Method
Author(s): Liwu W. Chang
E-mail Address: liwu@aic.nrl.navy.mil
Citation: Proceedings of the 9th Florida AI Research Symposium, Key West, Florida.
Date: May 20-22, 1996
Report No.: AIC-96-025

Abstract

In this paper, we describe methods for a clustering system in the context of a graphic model from two aspects. The first aspect is about the properties of the proposed clustering method, and the second aspect is on graph structure-based interpretation. We present methods for dynamically adjusting contents of clusters in the appearance of new samples. The result of clustering is regarded as a latent variable in the existing graph model. Clustering criteria are evaluated based on statistical properties of the graph model. To enhance the clarity in interpretation, we organize instances according to highly correlated features. We use an example to show the merits of using a graph model.

Title: A Proposal for Refining Case Libraries
Author(s): David W. Aha
E-mail Address: aha@aic.nrl.navy.mil
Citation: In R. Bergmann and W. Wilke (Eds.). Fifth German Workshop on Case-Based Reasoning: Foundations, Systems, and Applications (Technical Report LSA-97-21E). Kaiserslautern, Germany: University of Kaiserslautern, Centre for Learning Systems and Applications, pp11-20
Date: 1996
Report No.: AIC-96-028

Abstract

Conversational case-based reasoning (CCBR) systems are used in many commercial applications. Their distinguishing behavior is that they interactively acquire features values from users (i.e., they incrementally build queries), and typically address problem diagnosis tasks. Users want CCBR systems to be *precise* (i.e., retrieve the correct case for solving their problem) and *efficient* (i.e., require a minimal amount of interaction before cases are retrieved). Case authors require substantial expertise to ensure that their case libraries satisfy these demands. Commercial CCBR vendors help by supplying documents describing guidelines for designing case libraries, but mastering them involves a challenging learning curve. Software is needed that helps authors to design and refine case libraries according to these design guidelines. This paper outlines a proposal for using machine learning and data mining techniques to support the process of case authoring by refining case libraries.

Intelligent M4 Systems

abstracts 1996

INTELLIGENT M4 SYSTEMS

Title: A Collaborative Model of Feedback in Human-Computer Interaction
Author(s): Manuel A. Pérez-Quiñones and John L. Sibert
E-mail Address: perez@aic.nrl.navy.mil
Citation: Internal Report (Submitted for publication to Conference on Human Factors in Computing Systems, CHI '96)
Date: 1996
Report No.: AIC-96-001

Abstract

Feedback plays an important role in human-computer interaction. It provides the user with evidence of closure, thus satisfying the communication expectations that users have when engaging in a dialogue. In this paper we present a model identifying five feedback states that must be communicated to the user to fulfill the communication expectations of a dialogue. The model is based on a linguistics theory of conversation, but is applied to a graphical user interface. An experiment is described in which we test users' expectations and their behavior when those expectations are not met. The model subsumes some of the temporal requirements for feedback previously reported in the human-computer interaction literature.

Title: Negotiating User-Initiating Cancellation and Interruption Requests
Author(s): Manuel A. Pérez-Quiñones and John L. Sibert
E-mail Address: perez@aic.nrl.navy.mil
Citation: Submitted for publication as a short paper to Conference on Human Factors in Computing Systems (CHI'96)
Date: April 14-18, 1996
Report No.: AIC-96-002

Abstract

Interruptions and cancellations are important parts of a user interface, yet they are treated as special cases in user interface design and notations. In an effort to build a dialogue notation that allows for effective definition of these commands or user turns, we present a behavioral definition of interruptions and cancellations. We show several examples of how our definition accounts for different forms of behavior. The behavioral definitions provided here are a step towards providing better support for the definition and implementation of these turns.

Title: The Message in the Medium: On the Functionality of It-clefts in Selected Discourses
Author(s): Dennis Perzanowski and John Gurney
E-mail Address: dennisp@aic.nrl.navy.mil
Citation: Internal Report
Date: February 20, 1996
Report No.: AIC-96-011

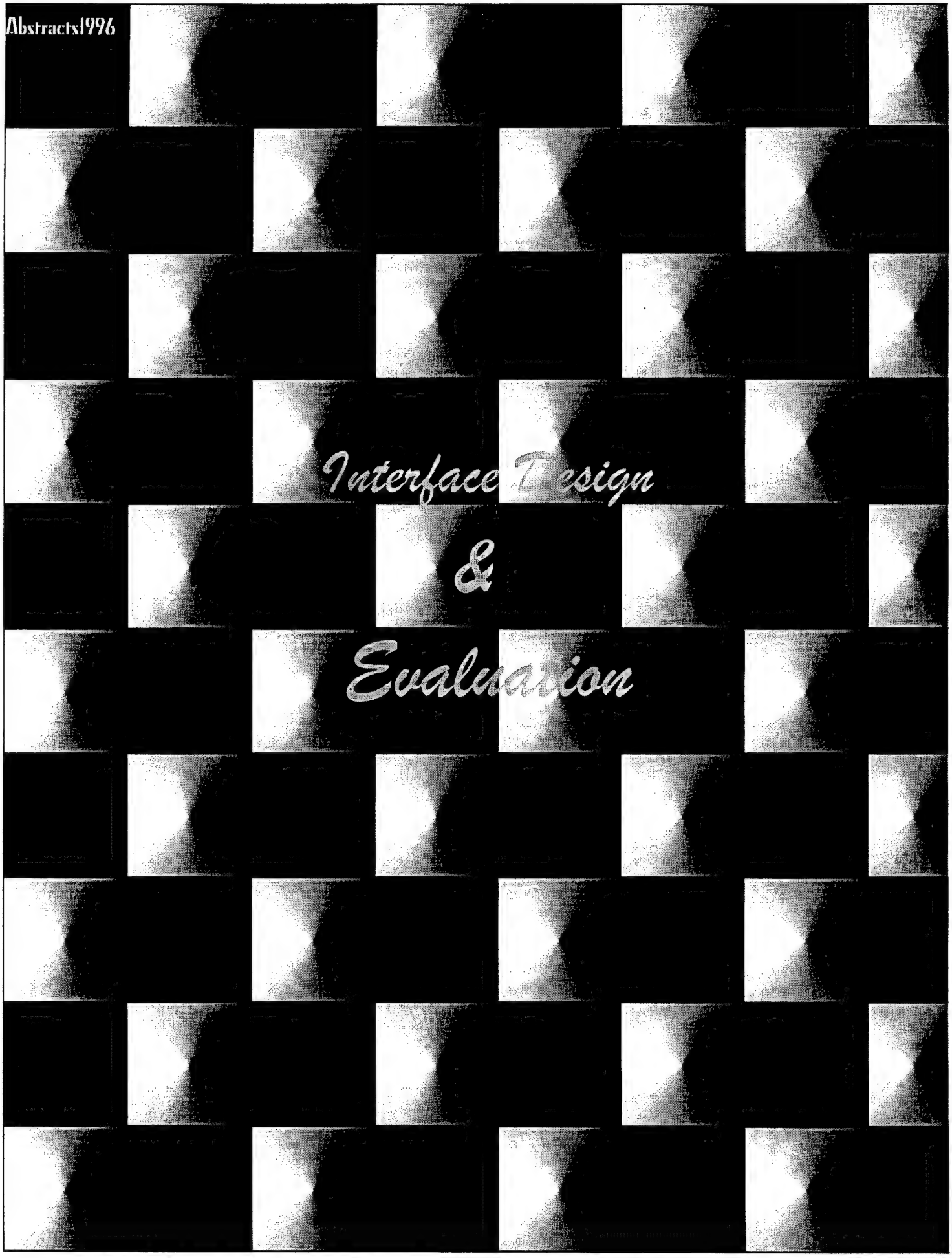
Abstract

Information in a discourse can be obtained by analyzing several different linguistic properties of the discourse. Various syntactic and semantic triggers provide clues to the complex informational structure of a discourse. For the purposes of this investigation, we selected several discourses taken from a series of wire service messages dealing with terrorist incidents that occurred in Central America from 1989 to 1991. The corpus is known as the "MUC-3" corpus. Because of their inferential properties, we identified it-cleft constructions in the corpus. We argue that, despite their rarity in the corpus under investigation, it-clefts provide additional information, and do not just contrast or emphasize focused linguistic material, such as noun or prepositional phrases. By substituting so-called "normal" word order, or SVO paraphrases, for the it-clefts in the messages, we determined what information the it-cleft sentences provided in the discourse. Our investigation reveals that, as a subset of the information that can be obtained in a discourse, it-clefts can be used to avoid conflicting or differing interpretations inherent in their SVO paraphrases, thereby minimizing possible confusion regarding the interpretation of what the author is trying to communicate. In some cases the speaker/writer's point of view or attitude about the subject matter being discussed is also revealed. For example, we show how a focused generic noun phrase in an it-cleft sentence provides a clearer statement of the author's intended meaning.

Title: Multimodal Interaction With a Map-Based Simulation
Author(s): Kenneth Wauchope
E-mail Address: wauchope@aic.nrl.navy.mil
Citation: Internal Report
Date: July 1996
Report No.: AIC-96-027

Abstract

This report describes InterLACE, a natural language and graphical interface to the LACE map-based military simulation system from Rome Air Development Center. InterLACE was built to serve as a research testbed for exploring issues in multimodal human-computer interaction, the linguistics of 2-D spatial relations in computerized map-based decision aids, and how the naturalness of the human-computer dialog in multimodal interfaces might be improved by applying principles of human-human discourse understanding. The system consists of a mouse-sensitive graphical map display built using the Gamet X Windows package from Carnegie Mellon University, the Navy AI Center's NAUTILUS general-purpose natural language processor, and commercial front and back ends for speaker-independent continuous speech recognition and open-vocabulary speech synthesis. Users can query information from the system's extensive real-world cartographic database of central Germany and issue route instructions to a simulated on-road ground vehicle. To date, InterLACE has been used at the AI Center as a platform for investigating natural language generation techniques and for an experimental study of the relative advantages of graphical versus natural language instructions in user task performance.


Interface Design
&
Evaluation

INTERFACE DESIGN AND EVALUATION

Title: Content Analysis of Communication in a Hierarchical Navy Team
Author(s): Lisa B. Achille and Kay G. Schulze
E-mail Address: achille@itd.nrl.navy.mil
Citation: Naval Research Laboratory Formal Report, NRL/FR/5510--96-9775
Date: February 13, 1996
Report No.: AIC-96-010

Abstract

Communications are a crucial aspect of military decision making. Team members in the AEGIS Combat Information Center (CIC) share information through verbal communication, computerized combat systems, and computerized displays. The authors recorded the internal CIC communications during AEGIS team training exercises and developed a classification scheme to categorize team communication. Speech turns were identified, classified, and analyzed. Individual classifications were grouped into categories to describe functional activities, including CIC activity, situation awareness, planning, acknowledgments, overload, and team coordination. With training, decision makers in large military teams take a different approach to planning and to the use of commands than do their counterparts in aircrews. A team member's position in the hierarchical structure influences his level of participation in each of the functional activities. The results suggest areas for further research to reduce communication network load and improve the efficiency of future command and control interface designs.

Title: Situation Assessment Through Collaborative Human-Computer Interaction
Author(s): Scott D. Kushnier, Christol H. Heithacker, James A. Ballas, and Daniel C.. McFarlane
E-mail Address: ballas@aic.nrl.navy.mil or mcfarlan@itd.nrl.navy.mil
Citation: In Naval Engineers Journal, July 1996, Vol .108, No. 4, pp41-51
Date: July 1996
Report No.: AIC 96- 023

Abstract

Data fusion has been characterized as taking place at four levels of abstraction: the unit level, the situation level, the threat level, and the resource allocation level. A unit level characterization tries to put down the attributes of individual platform objects. At the situation level, organized groups of units, such as battle groups, are explored. At the threat level and resource allocation level, reasoning about possible enemy intentions and possible responses is undertaken. Little work, however, has been done concerning some of the higher levels of abstraction, namely the force and threat levels. This paper presents an approach toward situation assessment which includes explicit conceptualizations of forces and threats. Graphical representations of these forces and threats are designed to enhance the unit level depiction without obscuring it. This paper

explores a novel style of user interface--one designed to allow collaboration between the person and the machine, enabling a tactical assessment which is superior to one in which either the person or the machine works in isolation. The paper will then describe a natural division of responsibilities between person and machine and illustrate the benefit of such a collaborative system in light of an example based on a warfare scenario.

Title: Shipboard VR: From Damage Control to Design
Author(s): Lawrence Rosenblum, Jim Durbin, Uput Obeysekare, Linda Sibert, David Tate, James Templeman, Joyti Agrawal, Daniel Fasulo, Thomas Meyer, Greg Newton, and Amit Shaley
E-mail Address: rosenblum@ait.nrl.navy.mil or durbin@ait.nrl.navy.mil or sibert@itd.nrl.navy.mil or tate@ait.nrl.navy.mil or templema@itd.nrl.navy.mil
Citation: IEEE Computer Graphics and Applications, November 1996, pp10-13
Date: November 1996
Report No.: AIC-96-032

Abstract

Virtual reality efforts in the Information Technology Division of the Naval Research Laboratory (NRL) span mission planning, rehearsal, and execution; simulation-based design, and medicine. We devote much of our work to ship-based applications, presenting two such efforts in this article. One project focuses on experiments in shipboard firefighting to verify the effectiveness of VR as a mission planning tool. The other project involves visualizing a preliminary design of a new Navy ship. Since that work did not extend into the actual design cycle, we can't quantify the results in terms of hours gained or costs saved. However, the design team and the program managers agreed that the VR visualization was worthwhile and provided a better understanding of the design.

Title: Individual Differences in Word Processing Strategies
Author(s): J.G. Temple and Astrid Schmidt-Nielsen
E-mail Address: schmidtn@aic.nrl.navy.mil
Citation: Book chapter in Psychology Beyond the Threshold: A Festschrift for William N. Dember. R. Hoffman and J.S. Sherrick (Eds.). American Psychological Association, Washington, DC, 1996
Date: 1996
Report No.: AIC-96-033

Abstract

The career of William N. Dember spans many research areas, not the least of which is the study of individual differences. Clearly, individuals differ from each other along a wide variety of dimensions: intelligence, field dependence, optimism/pessimism, working memory span, etc. However, the manner in which such individual differences affect the types of strategy choices people make is less obvious. Dember and Earl (1957) argued that individuals as well as environmental stimuli possess a complexity value. When the complexity value of a situation far exceeds an individual's own complexity value, the stimulus may become aversive to the individual and anxiety-provoking. Individuals are motivated to choose novel or complex stimuli when they fall within a comfortable

range of their own complexity levels. Commonly referred to as the Dember and Earl Theory of Choice (DETC), this model has important implications for research on individual differences, particularly for any type of individual difference that might serve as an indicator of complexity itself. For example, a person with excellent cognitive abilities might be expected to pursue more intellectually challenging tasks than someone with poorer abilities. While the DETC originated in the animal laboratory, its influence on individual differences research extends well beyond the T-maze.

In this chapter, we will examine some of the individual difference in cognition that may be associated with the type of strategy choices people make when interacting with computers. In what follows, we will describe some of the research that has been conducted on the role of individual differences in computer usage. We shall then consider a study of Schmidt-Nielsen and Ackerman (1993) that examined the preference for keyboard shortcuts versus pulldown menus commonly found on today's graphical user interface (GUI) computer systems as reflecting two general type of strategies (lookup versus memory retrieval) that people may adopt when completing highly receptive tasks that possess two alternative ways to accomplish the same function, but that differ in their relative efficiency and difficulty to master. Using a computer application that was unfamiliar to users, they found that choice of strategy paralleled the strategy adopted by the same participants on a simple laboratory task that was also highly repetitive. We shall then discuss in detail a new study intended to further explore the issues raised by the results of Schmidt-Nielsen and Ackerman (1993), using participants across a broad range of experience and with a common computer application (word processing). Important questions were whether participants who engaged in a lookup strategy on the simple laboratory task also used a lookup strategy when word processing (used primarily pulldown menus), whether the choice of strategy is related to individual differences in cognitive resource management, and how these effects interact with experience. Finally, we shall discuss the results of the study in terms of the Schmidt-Nielsen and Ackerman results and the complex relations between individual differences in cognition and experience, and will conclude with how these results might be explained by the DETC.

Title: Speaker Recognizability Testing for Voice Coders
Author(s): Astrid Schmidt-Nielsen and Derek Brock
E-mail Address: schmidtn@aic.nrl.navy.mil or brock@itd.nrl.navy.mil
Citation: Proceedings of ICASSP-96, Atlanta, GA, May 1996, vol. II, pp1149-1152
Date: May 1996
Report No.: AIC-96-034

Abstract

Users of low data rate voice coders now demand good speaker recognition in addition to quality and intelligibility. Speaker recognizability was one of the selection criteria for the DoD Digital Voice Processor Consortium in selecting a new standard 2400 bps algorithm. We have developed a speaker recognition test based on SAME-DIFFERENT judgments for pairs of sentences spoken by 10 male and 10 female speakers. Preliminary experiments showed that the sensitivity of the test is similar to that of currently used acceptability and

intelligibility tests. Male and female talkers produced somewhat different rank orderings, but averaging over males/females gave results that "make sense" when compared with intelligibility and acceptability scores for the same coders. The results of these experiments determined the speaker recognition test procedures that were used in the 2400 bps coder final selection process

---

Title: Perceiving Talker Differences
Author(s): Astrid Schmidt-Nielsen
E-mail Address: schmidtn@aic.nrl.navy.mil
Citation: Abstract submitted for the November 1996 meeting of the Psychonomic Society; appears in Abstracts of the Psychonomic Society, 1996, v1, p55
Date: 1996
Report No.: AIC-96-035

Abstract

Talker discrimination for two sets of talkers, 10 males and 10 females, was evaluated using paired comparisons. Measured voice characteristics (fundamental frequency, talking rate, etc.) were related to voice discriminability (d') and to dissimilarity ratings. The voice characteristics that were best related to listener discriminations differed for the male and female talker sets, and listeners from different parts of the country perceived the talker space differently.

Title: Characterizing Human Ability To Discriminate Talkers Over Low Data Rate Voice Coders
Author(s): Astrid Schmidt-Nielsen
E-mail Address: schmidtn@aic.nrl.navy.mil
Citation: Abstract appears in Journal of the Acoustical Society of America, 1996, v100, p2762
Date: 1996
Report No.: AIC-96-036

Abstract

Talker discrimination over low data rate voice coders (2400 bits/s) was evaluated in three separate experiments using a paired comparison task. Test materials were Harvard sentences spoken by ten male and ten female talkers from the Boston area. Listeners were asked to decide whether two different sentences were spoken by the same person or by two different people. They then judged how dissimilar the two voices were using a five-point scale. The ability to discriminate among the voices (measured by *d'*) was compared to the subjective judgments of the perceptual distance between the voices. The effect of different types of voice coders on talker discriminability and on the perceived talker space was compared with uncoded speech. Comparisons with traditional measures of intelligibility and voice quality suggest that higher intelligibility or quality scores are not necessarily related to better talker discrimination, but dissimilarity ratings of different talkers were more closely related to voice quality scores. Listeners from two different parts of the country also perceived the talker space differently. [Work supported by NAVSPAWARSYSCOM.]

Title: Interfaces for Intelligent Control of Data Fusion Processing
Author(s): James A. Ballas, Daniel C. McFarlane, Lisa B. Achille, Janet L. Stroup, C.H. Heithecker, and S.D. Kushnier
E-mail Address: ballas@aic.nrl.navy.mil or mcfarlan@itd.nrl.navy.mil or achille@itd.nrl.navy.mil or stroup@itd.nrl.navy.mil
Citation: Naval Research Laboratory Formal Report, NRL/FR/5510--96-9806
Date: 1996
Report No.: AIC-96-037

Abstract

An approach to support the collaboration between human and computer in achieving data fusion and situation assessment was developed conceptually and implemented in a software prototype. This approach supports communication of inductive assessments from the user to an intelligent computer capable of recommending actions on the basis of tactical doctrine as well as examining tactical relations (e.g., potential threats to a particular asset) in the knowledge base. The prototype extends certain concepts of an intelligent control architecture called KOALAS (Knowledgeable, Observation Analysis-Linked Advisory System) to higher levels of data fusion (i.e., situation assessment of forces and threats). The interface includes graphical components for hypothesis and advisory representations and interactive at the object, force, and threat levels of data fusion. The interface representations and interaction at the force and threat level are a particularly innovative aspect of this work. The prototype implements human-computer functional allocation based upon the principle for deductive/inductive logic operations. An important principle in the interface design was to support as much interaction as possible within a tactical window. The design of this prototype was based upon an analysis of issues raised in current approaches to automation and intelligent control, on analyses of collaborative data fusion in a relevant tactical scenario, and an analysis of AEGIS voice communication concerning data fusion. The implementation of the prototype included the development of a hierarchical, object-oriented knowledge base and a rule base that can reason about forces and threats.

Title: Computations Modeling of Multimodal I/O in Simulated Cockpits
Author(s): James A. Ballas
E-mail Address: ballas@aic.nrl.navy.mil
Citation: In Proceedings of the Third International Conference on Auditory Display. S. P. Frysinger and G. Kramer (Eds.). Xerox Palo Alto Research Center, Palo Alto, CA, Nov. 4-6, 1996, pp135-136.
Date: November 4-6, 1996
Report No.: AIC-96-038

Abstract

The objective of this research is to qualify and model the effects of multimodal input and output in a multitask experiment, using a low fidelity cockpit simulation. The empirical assessment will address the effects of shifting some of the information presented to the user from the visual modality to the auditory modality. This will include the use of both speech and non-speech sounds. The modeling work will develop and assess computational models of the peripheral

perceptual/motor control and central cognitive information processing involved in the multitask experiment, with the objective of developing accurate simulation of human performance under the same simulated conditions.

Machine Learning

MACHINE LEARNING

Title: A Review and Comparative Evaluation of Feature Weighting Methods for Lazy Learning Algorithms
Author(s): Dietrich Wettschereck, David W. Aha, and Takao Mohri
E-mail Address: aha@aic.nrl.navy.mil
Citation: In Artificial Intelligence Review, v11, n1-5, February 1997, pp273-314
Date: 1996
Report No.: AIC-96-006

Abstract

Most lazy learning algorithms are derivatives of the k-nearest neighbor (k-nearest neighbor) classifier, which uses a distance function to generate predictions from stored instances. Several studies have shown this algorithm to be highly sensitive to the definition of its distance function. Many k-nearest neighbor variants have been proposed to reduce this sensitivity, and most do so by parameterizing the distance function with attribute weights. These proposed parameter-setting methods have not been empirically compared. This paper includes a review of weight-setting methods and their empirical comparison. We summarize these results with five hypotheses and provide empirical evidence to support each. Our investigation revealed that most methods correctly assign low weights to completely irrelevant attributes. Furthermore, methods that use performance feedback to assign weight settings demonstrated three advantages over other methods: they require less pre-processing, perform better in the presence of interacting attributes, and generally require less training data to learn good settings.

Title: Continuous Localization Using Evidence Grids
Author(s): Alan C. Schultz, William Adams, and John J. Grefenstette
E-mail Address: schultz@aic.nrl.navy.mil or adams@aic.nrl.navy.mil or gref@aic.nrl.navy.mil
Citation: Internal Report
Date: December 1996
Report No.: AIC-96-007

Abstract

The evidence grid representation provides a uniform representation for fusing temporally and spatially distinct sensor readings. However, the use of evidence grids requires that the robot be localized within its environment. Odometry errors typically accumulate over time, making localization estimates degrade, and introducing significant errors into evidence grids as they are built. We have addressed this problem by developing a new method for "continuous localization," in which the robot corrects its localization estimates incrementally. Assuming the mobile robot has a map of its environment represented as an evidence grid, localization is achieved by building a series of "local evidence grids" based on current odometry and registering the local and global grids. The registration produces an error estimate which is used to correct the odometry results are given on the effectiveness of alternative registration methods (i.e.,

gradient search, randomized search, genetic algorithms), and quantify the improvement of continuous localization over periodic localization methods.

Title: A NN Algorithm for Boolean Satisfiability Problems
Author(s): William M. Spears
E-mail Address: spears@aic.nrl.navy.mil
Citation: Proceedings of the 1996 IEEE International Conference on Neural Networks, Washington DC, pp1121-1126
Date: June 1996
Report No.: AIC-96-009

Abstract

Satisfiability (SAT) refers to the task of finding a truth assignment that makes an arbitrary Boolean expression true. This paper compares a neural network algorithm (NNSAT) with GSAT [Selman, 1992], a greedy algorithm for solving satisfiability problems. GSAT can solve problem instances that are difficult for traditional satisfiability algorithms. Results suggest that NNSAT scales better as the number of variables increase, solving at least as many hard SAT problems.

Title: A Comparison of Action Selection Learning Methods
Author(s): Diana Gordon and Devika Subramanian
E-mail Address: gordon@aic.nrl.navy.mil
Citation: Proceedings of the Third International Workshop on Multistrategy Learning, pp95-102
Date: July 1996
Report No.: AIC-96-012

Abstract

Our goal is to develop a hybrid cognitive model of how humans acquire skills on complex cognitive tasks. We are pursuing this goal by designing hybrid computational architectures for the NRL Navigation task, which requires competent sensorimotor coordination. In this paper, we empirically compare two methods for control knowledge acquisition: reinforcement learning and a novel variant of action models, as well as a hybrid of these methods, with human learning on this task. Furthermore, we experimentally demonstrate the impact of background knowledge on system performance. Our results indicate that the performance of our action models approach more closely approximates the rate of human learning on this task than does reinforcement learning.

Title: Cognitive Modeling of Action Selection Learning
Author(s): Diana Gordon and Devika Subramanian
E-mail Address: gordon@aic.nrl.navy.mil
Citation: Proceedings of the Eighteenth Annual Conference of the Cognitive Science Society, pp546-551
Date: May 1996
Report No.: AIC-96-013

Abstract

Our goal is to develop a hybrid cognitive model of how humans acquire skills on complex cognitive tasks. We are pursuing this goal by designing hybrid computational architectures for the NRL Navigation task, which requires competent sensorimotor coordination. In this paper, we empirically compare two methods for control knowledge acquisition: reinforcement learning and a novel variant of action models, with human learning on this task. Furthermore, we experimentally demonstrate the impact of background knowledge on system performance. Our results indicate that the performance of our action models approach more closely approximates the rate of human learning on this task than does reinforcement learning.

Title: Proportional Selection and Sampling Algorithms
Author(s): John J. Grefenstette
E-mail Address: gref@aic.nrl.navy.mil
Citation: Book chapter in The Handbook of Evolutionary Computation, T. Baeck, D. Fogel and Z. Michalewicz (Eds.), IOP Publishing and Oxford University Press
Date: 1997
Report No.: AIC-96-018

Abstract

Proportional Selection assigns to each individual a reproductive probability that is proportional to the individual's relative fitness. This section presents the proportional selection method as a series of steps: (1) map the objective function to fitness, (2) create a probability distribution proportional to fitness, and (3) draw samples from this distribution. Characterizations of selective pressure, fitness scaling techniques, and alternative sampling algorithms are also presented.

Title: Rank-based Selection
Author(s): John J. Grefenstette
E-mail Address: gref@aic.nrl.navy.mil
Citation: Book chapter in The Handbook of Evolutionary Computation, T. Baeck, D. Fogel and Z. Michalewicz (Eds.), IOP Publishing and Oxford University Press
Date: 1997
Report No.: AIC-96-019

Abstract

Rank-based selection assigns a reproductive or survival probability to each individual that depends only on the rank ordering of the individuals in the current population. The section presents a brief discussion of ranking, including linear, nonlinear, (μ, λ) and $(\mu + \lambda)$ methods. The theory of rank-based selection is briefly outlined, including a discussion of implicit parallelism and characterizations of selective pressure in rank-based evolutionary algorithms.

Title: Efficient Implementation of Algorithms
Author(s): John J. Grefenstette
E-mail Address: gref@aic.nrl.navy.mil
Citation: Book chapter in The Handbook of Evolutionary Computation, T. Baeck, D. Fogel and Z. Michalewicz (Eds.), IOP Publishing and Oxford University Press
Date: 1997
Report No.: AIC-96-020

Abstract

This section discusses techniques for the efficient implementation of evolutionary algorithms, including generating random numbers, implementing the genetic operators, and reducing computational effort in the evaluation phase.

Title: Methods for Competitive and Cooperative Co-evolution
Author(s): John J. Grefenstette and Robert Daley
E-mail Address: gref@aic.nrl.navy.mil or daley@itd.nrl.navy.mil
Citation: In Adaptation, Co-evolution and Learning in Multiagent Systems: Papers from the 1996 AAAI Symposium, 45-50, Technical Report SS-96-01, Menlo Park, CA: AAAI Press
Date: March 1996
Report No.: AIC-96-021

Abstract

We have been investigating evolutionary methods to design behavioral strategies for intelligent robots in multi-agent environments. Such environments resemble an ecological system in which species evolve and adapt in a complex interaction with other evolving and adapting species. This paper will report on our investigations of alternative co-evolutionary approaches in the context of a simulated multi-agent environment.

Title: Genetic Learning for Adaptation in Autonomous Robots
Author(s): John J. Grefenstette
E-mail Address: gref@aic.nrl.navy.mil
Citation: Robotics and Manufacturing: Recent Trends in Research and Applications, Vol. 6, M. Jamshidi, F. Pin and P. Dauchez (Eds.), Proceedings of the Sixth International Symposium on Robotics and Manufacturing, New York: ASME Press, pp265-270
Date: May 1996
Report No.: AIC-96-022

Abstract

This paper deals with problems arising in robots that are expected to perform autonomously for extended periods. An important problem for such systems is how to adapt the robot's rules of behavior in response to changes in its own capabilities. If the robot finds that some sensors or some basic actions are no longer available, perhaps due to a problem with its hardware or due to some undetected environmental cause, then the robot must learn new rules for performing its mission that use whatever remaining capabilities are still available.

This paper presents an approach called "Anytime Learning" that enables a robot to gracefully adapt to its current capabilities.

Title: Cloud Classification Using Error-Correcting Output Codes
Author(s): David W. Aha and Richard L. Bankert (Marine Meteorology Division, Naval Research Laboratory, Monterey, CA 93943)
E-mail Address: aha@aic.nrl.navy.mil or bankert@nrlmry.navy.mil
Citation: To appear in AI Applications: Natural Resources, Agriculture, and Environmental Science
Date: October 1996
Report No.: AIC-96-024

Abstract

This paper describes novel artificial intelligence methods for classifying 16x16 pixel regions (obtained from AVHRR images) in terms of cloud type (e.g., stratus, cumulus, etc.). We previously reported that intelligent feature selection methods, combined with nearest neighbor classifiers, can dramatically improve classification accuracy on this task. Our subsequent analyses of the confusion matrices revealed that a small number of confusable classes (e.g., cirrus and cirrostratus) dominated the classification errors. We conjectured that, if the class labels in the data were re-represented so that these cloud classes are more easily distinguished, then additional accuracy gains might result. We explored this hypothesis by replacing each class label with a set of "error-correcting output codes," a general technique applicable to any classification algorithm for tasks with at least three classes. Our initial results are promising; error correcting codes significantly increased classification accuracy compared with using standard representations for class labels. To our knowledge, this is the first successful integration of k-nearest neighbor classifiers and error-correcting output codes (i.e., where k is, effectively, small). The primary contributions of this paper to environmental scientists are the description of how to apply error-correcting output codes to environmental science tasks, and a promising application concerning cloud classification. We also explain why environmental scientists should always select, for their classification tasks, a classifier that reduces both variance and learning bias.

Title: RoboShepherd: Learning a Complex Behavior
Author(s): Alan C. Schultz, John J. Grefenstette, and William Adams
E-mail Address: schultz@aic.nrl.navy.mil or gref@aic.nrl.navy.mil or adams@aic.nrl.navy.mil
Citation: Proceedings of the Robots and Learning Workshop, FLAIRS, pp105-113, May 20, 1996
Date: May 1996
Report No.: AIC-96-030

Abstract

This paper reports on recent results using genetic algorithms to learn decision rules for complex robot behaviors. The method involves evaluating hypothetical rule sets on a simulator and applying simulated evolution to evolve more effective rules. The main contributions of this paper are (1) the task learned is a complex

behavior involving multiple mobile robots, and (2) the learned rules are verified through experiments on operational mobile robots. The case study involves a shepherding task in which one mobile robot attempts to guide another robot to a specified area. (This paper is an expanded version of the following paper from ISRAM96.)

Title: Robo-Shepherd: Learning Complex Robotic Behaviors
Author(s): Alan C. Schultz, John J. Grefenstette, and William Adams
E-mail Address: Schultz@aic.nrl.navy.mil or gref@aic.nrl.navy.mil
Citation: Robotics and Manufacturing: Recent Trends in Research and Applications, Vol. 6, M. Jamshidi, F. Pin and P. Dauchez (Eds.), Proceedings of the Sixth International Symposium on Robotics and Manufacturing, New York: ASME Press, pp763-768
Date: May 1996
Report No.: AIC-96-031

Abstract

This paper reports on recent results using genetic algorithms to learn decision rules for complex robot behaviors. The method involves evaluating hypothetical rule sets on a simulator and applying simulated evolution to evolve more effective rules. The main contributions of this paper are (1) the task learned is a complex behavior involving multiple mobile robots, and (2) the learned rules are verified through experiments on operational mobile robots. The case study involves a shepherding task in which one mobile robot attempts to guide another robot to a specified area.

Title: Recombination Parameters
Author(s): William M. Spears
E-mail Address: spears@aic.nrl.navy.mil
Citation: Book chapter in The Handbook of Evolutionary Computation, T. Baeck, D. Fogel and Z. Michalewicz (Eds.), IOP Publishing and Oxford University Press
Date: 1997
Report No.: AIC-96-039

Abstract

One operator that is often used in evolution strategies, genetic algorithms, and genetic programming is recombination, where material from two (or more) parents is used to create new offspring. There are numerous ways to implement recombination. This section will focus mainly on recombination operators that construct potentially useful solutions to a problem from smaller components (often called "building blocks"). Recombination operators that "blend" are discussed in section XXX. This section gives an overview of some of the motivation, issues, theory, and heuristics for "building block" recombinations.

Title: Speciation Methods
Author(s): Kalyanmoy Deb and William M. Spears
E-mail Address: spears@aic.nrl.navy.mil
Citation: Book chapter in The Handbook of Evolutionary Computation, T. Baeck, D. Fogel and Z. Michalewicz (Eds.), IOP Publishing and Oxford University Press
Date: 1997
Report No.: AIC-96-040

Abstract

In nature, a species is defined as a collection of phenotypically similar individuals. Many biologists believe that individuals in a sexually reproductive species can be created and maintained by allowing restrictive mating only among individuals from the same species. The connection between the formation of multiple species in nature and in search and optimization problems lies in solving multimodal problems, where the objective is not only to find one optimal solution, but to find a number of optimal solutions. In those problems, each optimal solution may be assumed to constitute a species. Since evolutionary algorithms work with a population of solutions, the concept of natural speciation techniques can be implemented to allow formation of multiple subpopulations, each forcing its search for one optimal solution. This way, multiple optimal solutions can be discovered simultaneously. In this section, a number of speciation techniques are discussed.

Title: Analyzing GAs Using Markov Models with Semantically Ordered and Lumped States
Author(s): William M. Spears and Kenneth A. De Jong
E-mail Address: spears@aic.nrl.navy.mil
Citation: In Foundations of Genetic Algorithms, R. Belew and M. Vose (Eds.), Morgan Kaufmann
Date: 1997
Report No.: AIC-96-041

Abstract

At the previous FOGA workshop, we presented some initial results on using Markov models to analyze the transient behavior of genetic algorithms (GAs) being used as function optimizers (GAFOs). In that paper, the states of the Markov model were ordered via a simple and mathematically convenient lexiographic ordering used initially by Nix and Vose. In this paper, we explore alternative orderings of states based on interesting semantic properties such as average fitness, degree of homogeneity, average attractive force, etc. We also explore lumping techniques for reducing the size of the state space. Analysis of those reordered and lumped Markov models provides new insights into the transient behavior of GAs in general and GAFOs in particular.

Title: Improvement To a Neural Network Cloud Classifier
Author(s): R.L. Bankert and David W. Aha
E-mail Address: aha@aic.nrl.navy.mil
Citation: Journal of Applied Meteorology, v35,n11, 1996, pp2036-2039
Date: 1996
Report No.: AIC-96-042

Abstract

Examination of various feature selection algorithms has led to an improvement in the performance of a probabilistic neural network (PNN) cloud classifier. These algorithms reduce the number of network inputs by eliminating redundant and/or irrelevant features (spectral, textural, and physical measurements.) One such algorithm, selecting 11 of the 204 total features, provides a 7% increase in PNN overall accuracy compared to an earlier version using 15 features. This algorithm employs the same search procedure as before, but a different evaluation function than used previously, which provides a similar bias to that of the PNN classifier. Noticeable accuracy improvements were also evident in individual cloud-type classes.

Title: Simulated Annealing for Hard Satisfiability
Author(s): William M. Spears
E-mail Address: spears@aic.nrl.navy.mil
Citation: Cliques, Coloring, and Satisfiability: Second DIMACS Challenge, D.S. Johnson and M.A. Trick (Eds.), DIMACS Series on Discrete Mathematics and Theoretical Computer Science, pp533-558
Date: 1996
Report No.: AIC-96-043

Abstract

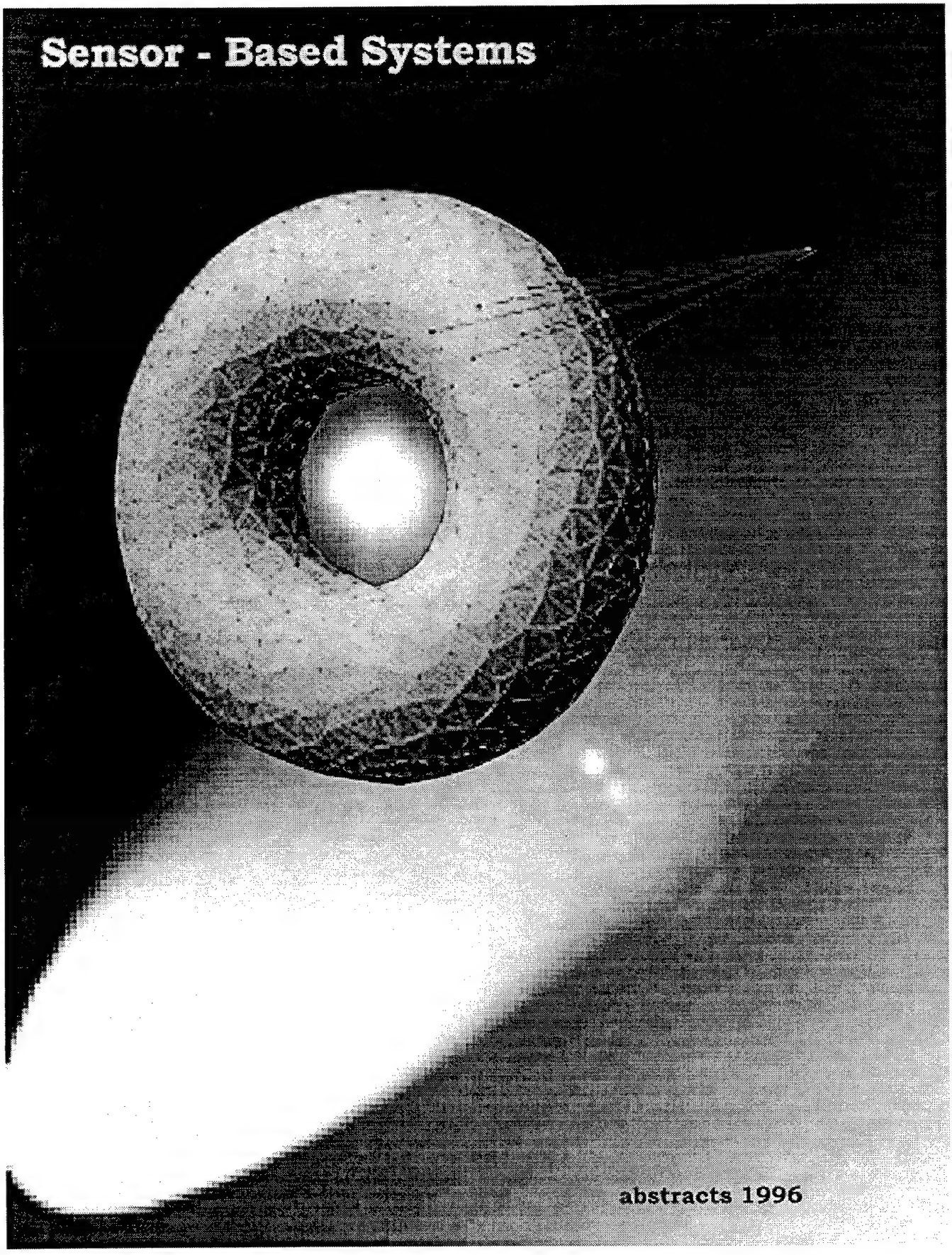
Satisfiability (SAT) refers to the task of finding a truth assignment that makes an arbitrary boolean expression true. This paper compares a simulated annealing algorithm (SASS) with GSA (Seaman, et al. 1992), a greedy algorithm for solving satisfiability problems. GSAT can solve problem instances that are extremely difficult for traditional satisfiability algorithms. Results suggest that SASAT scales up better as the number of variables increases, solving at least as many hard SAT problems with less effort. The paper then presents an ablation study that helps to explain the relative advantage of SASAT over GSAT. Next, an improvement to the basic SASAT algorithm is examined, based on a random walk implemented in GSAT (Selman and Kautz, 1993). Finally, we examine the performance of SASAT on a test suite of satisfiability problems produced by the 1993 DIMACS challenge.

Title: Workshop Report: Case-Based Reasoning
Author(s): David W. Aha
E-mail Address: aha@aic.nrl.navy.mil
Citation: AI Magazine, v17, Spring 1995, p92
Date: 1996
Report No.: AIC-96-044

Abstract

The 1994 Workshop on Case-Based Reasoning (CBR) focused on the evaluation of CBR theories, models, systems, and system components. The CBR community addressed the evaluation of theories and implemented systems, with the consensus that a balance between novel innovations and evaluations could maximize progress.

Sensor - Based Systems



abstracts 1996

SENSOR-BASED SYSTEMS

Title: Rejection with Multilayer Neural Networks: Screening Image Data
Author(s): Behrooz Kamgar-Parsi and Behzad Kamgar-Parsi
E-mail Address: kamgar@aic.nrl.navy.mil or behzad@ait.nrl.navy.mil
Citation: NRL Review, Naval Research Laboratory Publication, NRL/PU/5530--96-
Date: 1996
Report No.: AIC-96-003

Abstract

Existing neural networks are unable to reject unfamiliar patterns, and thus misclassify them as members of classes of patterns with which they are familiar. Indeed, other classifiers in the fields of computer vision, statistical pattern recognition, etc., also suffer from a similar shortcoming, as they can only find the closest class--which may or may not be the correct class. Hence, the use of neural networks, and other classifiers, for pattern recognition have been limited to controlled environments, i.e., environments that only involve a limited number of known classes of patterns (classes used in the design of the classifier), i.e., optical character recognition. In uncontrolled environments, encompassing many real life problems, however, there is no guarantee that all the patterns that will be presented to the network (or other classifiers) would actually belong to one of the classes on which the network has been trained. For application in such environments, current pattern recognition and computer vision techniques resort to some ad hoc thresholds in order to decide whether to accept or reject the unknown pattern as belonging to a certain class. This often produces unreliable results. We have developed a method to construct multilayer perceptrons with rejection capabilities for visual patterns that are meaningful to humans. The method is potentially applicable to a variety of problems which are of interest both to the Navy and the commercial sector.

Title: Model-based Pattern Recognition with Multilayer Neural Networks: Learning from the Eye
Author(s): Behrooz Kamgar-Parsi and Behzad Kamgar-Parsi
E-mail Address: kamgar@aic.nrl.navy.mil or behzad@ait.nrl.navy.mil
Citation: Submitted for publication to Neural Computation
Date: 1996
Report No.: AIC-96-017

Abstract

We propose a model-based pattern recognition approach using multilayer neural networks to overcome certain shortcomings of the existing model-based techniques. In certain domains, the approach may allow the possibility of duplicating the discriminating power of the human eye in a network, provided that the pattern in question is meaningful to humans. To facilitate this we have developed a random deformation technique capable of generating an arbitrarily large number of true and false look-alikes of the model. The suggested approach attempts to construct decision boundaries at places where the human

eye appears to "draw" the line between acceptable and unacceptable patterns. Application of this technique to a real life problem shows a performance comparable to that of the eye.

Title: Developing Multilayer Neural Networks for Environments of Interest to the Intelligence Community

Author(s): Behrooz Kamgar-Parsi and Behzad Kamgar-Parsi
E-mail Address: kamgar@aic.nrl.navy.mil or behzad@aic.nrl.navy.mil

Citation: Symposium on Advanced Information Processing, sponsored by Advanced Information Processing and Analysis Steering Group, Advanced Research and Development Committee, Intelligence Community, Sheraton Premiere Hotel, Tysons Corner, Virginia
Date: March 26-28, 1996
Report No.: AIC-96-029

Abstract

The information environment that the Intelligence Community has to deal with is typically uncontrolled, i.e., an environment that involves previously unseen data items -- with unknown features and attributes. The presence of such data items can render useless classifiers such as nearest neighbor, statistical and existing multilayer neural networks. This is because such classifiers are not capable of realizing that a given datum (or pattern) may be "strange" or unknown, and thus would (mis)classify it as a member of one of the classes of data with which they are familiar. For example, a neural network which is trained on the photos of a certain number of fugitives would classify the photos of every person as one of those fugitives. For applications in such environments, one needs a classifier which is capable of rejection as well as (correct) classification. We have developed a method to construct multilayer perceptions with rejection capabilities for visual patterns that are meaningful to humans. The application of this technique to a real life problem, namely discriminating images containing aircraft from the rest, has shown a performance comparable to that of the human eye.

1995 PUBLICATIONS

AIC-95-001 Stratified Case-Based Reasoning: Reusing Hierarchical Problem Solving Episodes, *L. Karl Branting and David W. Aha*

AIC-95-002 Extending the User Action Notation (UAN) for specifying Interfaces with Multiple Input Devices and Parallel Path Structure, *Lynn Dievendorf, Derek Brock, and Robert J.K. Jacob*

AIC-95-003 An Implementation and Experiment with the Nested Generalized Exemplars Algorithm, *David W. Aha*

AIC-95-004 For Every Generalization Action, Is There Really an Equal and Opposite Reaction? Analysis of the Conservation Law for Generalization Performance, *R. B. Rao, Diana F. Gordon, William M. Spears*

AIC-95-005 Unsupervised Classification Procedures Applied to Cloud Data, *Diana Gordon, Paul Tag, and Richard Bankert*

AIC-95-006 An Analysis of Communications and the Use of Military Terms in Navy Team Training, *Lisa B. Achille, Kay G. Schulze, and Astrid Schmidt-Nielsen*

AIC-95-007 Evaluation and Selection of Biases for Machine Learning, *Diana Gordon and Marie des Jardins*

AIC-95-008 Genetic Algorithms for Expert System Validation, *Edward A. Roache, Kenneth A. Hickok, Kenneth F. Loje, Michael W. Hunt, and John J. Grefenstette*

AIC-95-009 Automatic Target Extraction in Infrared Images, *Behrooz Kamgar-Parsi*

AIC-95-010 A Coevolutionary Approach to Learning Sequential Decision Rules, *Mitchell A. Potter, Kenneth A. De Jong, and John J. Grefenstette*

AIC-95-011 A Test of Speaker Recognition Using Human Listeners, *Astrid Schmidt-Nielsen*

AIC-95-012 Adaption of Knowledge for Reuse, *David Aha*, editor

AIC-95-013 Virtual Genetic Algorithms: First Results, *John Grefenstette*

AIC-95-014 Robot Learning with Parallel Genetic Algorithms on Networked Computers, *John Grefenstette*

AIC-95-015 Extending the User Action Notation for Research in Individual Differences, *Derek Brock, Lynn Dievendorf, Deborah Hix, and J. Greg Trafton*

AIC-95-016 Evolving Complex Structures via Cooperative Coevolution, *Kenneth A. De Jong and Mitchell A. Potter*

AIC-95-017 Evolving Neural Networks with Collaborative Species, *Mitchell A. Potter and Kenneth A. De Jong*

AIC-95-018 Mental Representations of Spatial Language, *Geoffrey S. Hubona, Stephanie S. Everett, Elaine Marsh, and Kenneth Wauchope*

AIC-95-019 A Paradigm to Assess and Evaluate Tools to Support the Software Development Process, *James. A. Ballas and Janet L. Stroup*

AIC-95-020 Interpreting the Language of Informational Sound, *James. A. Ballas*

AIC-95-021 Conversational Dialogue in Graphical User Interfaces: Interaction Technique Feedback and Dialogue Structure, *Manuel A. Pérez-Quiñones*

AIC-95-022 Applying Genetic Algorithms to the Testing of Intelligent Controllers, *Alan C. Schultz, John J. Grefenstette, and Kenneth A. De Jong*

AIC-95-023 Applying Machine Learning in Practice, *David Aha,* editor

AIC-95-024 A Testbed for Experiments in Adaptive Memory Retrieval and Indexing, *Li Wu Chang and Patrick Harrison*

AIC-95-025 Rejection of Unfamiliar Patterns with Multilayer Neural Networks, *Behrooz Kamgar-Parsi and Behzad Kamgar-Parsi*

AIC-95-026 Weighting Features, *Dietrich Wettschereck and David W. Aha*

AIC-95-027 Learning to Break Things: Adaptive Testing of Intelligent Controllers, *Alan C. Schultz, John J. Grefenstette, and Kenneth A. De Jong*

AIC-95-028 Computational Pragmatics in HCI: Use of Dialog Context in a Multimodal Application, *Manuel A. Pérez-Quiñones*

AIC-95-030 VEG: Intelligent Workbench for Studying Earth's Vegetation, *Patrick R. Harrison, P. Ann Harrison, and Daniel S. Kimes*

AIC-95-031 Performance Evaluation of Navigation Algorithms Using Percolation Theory, *Ralph Hartley*

AIC-95-032 Advanced Interaction for Command and Control Planning Systems, *Linda E. Sibert and James N. Templeman*

AIC-95-033 A Methodology for Developing New Interaction Techniques, *Deborah Hix, James N. Templeman, Ankush Gosain, and Kapil Dandekar*

AIC-95-034 Pre-screen Projection: From Concept to Testing of a New Interaction Technique, *Deborah Hix, James N. Templeman, and Robert J.K. Jacob*

AIC-95-035 Virtual Environment Firefighting / Ship Familiarization Feasibility Tests Aboard the EX-USS *Shadwell, David Tate, Linda E. Sibert, F. W. Williams, LCDR Tony King, and Donald H. Hewitt*

AIC-95-036 Ecological Acoustics: Which Ecology? What Acoustics?, *James A. Ballas*

AIC-95-037 Navy Team Communications for Tactical Decision Making, *Lisa B. Achille, and Kay G. Schulze*

AIC-95-038 Distribution and Moments of the Weighted Sum of Uniform Random Variables with Applications in Reducing Monte Carlo Simulations, *Behzad Kamgar-Parsi, Behrooz Kamgar-Parsi, and Menashe Brosh*

AIC-95-039 Rejection with Multilayer Neural Networks: Automatic Generation of the Training Set, *Behrooz Kamgar-Parsi and Behzad Kamgar-Parsi*

AIC-95-040 Coding and Compression with Flexible Transforms, *Behzad Kamgar-Parsi, Behrooz Kamgar-Parsi, and Larry Schuette*

AIC-95-041 Why Do Now What Can Be Done Later?, *Scott Musman and Liwu Chang*

AIC-95-042 Knack: An Adaptive CBR Tool for Experimenting with Retrieval and Indexing, *Liwu Chang, Patrick R. Harrison, and Laura Davis*

AIC-95-043 Adapting Crossover in Evolutionary Algorithms, *William M. Spears*

AIC-95-044 Recombination Parameters, *William M. Spears*

AIC-95-045 Evolving Fuzzy Logic Control Strategies Using SAMUEL: An Initial Implementation, *Helen Cobb and John J. Grefenstette*

AIC-95-046 Toward Specification Techniques for Pre-Screen Projection and Other Next-Generation User Interfaces, *Robert J.K. Jacob and James Templeman*

AIC-95-047 Explicitly Biased Generalization, *Diana Gordon and D. Perlis*

AIC-95-048 A Wide-field Triangulation Laser Rangefinder for Machine Vision, *Frank Pipitone and Thomas Marshall*

AIC-95-049 A Hybrid Model Using Neural Networks and ACT–R, *J. Gregory Trafton*

AIC-95-051 Model-based Pattern Recognition with Multilayer Neural Networks: Learning From the Eye, *Behrooz Kamgar-Parsi and Behrad Kamgar-Parsi*

AIC-95-052 On Decentralizing Selection Algorithms, *Kenneth De Jong and Jayshree Sarma*

1994 PUBLICATIONS

AIC-94-001 Predictive Models Using Fitness Distributions of Genetic Operators, *John J. Grefenstette*

AIC-94-002 Evolutionary Algorithms in Robotics, *John J. Grefenstette*

AIC-94-003 Learning Robot Behaviors Using Genetic Algorithms, *Alan C. Schultz*

AIC-94-004 Integrating Reactive, Sequential, and Learning Behavior Using Dynamical Neural Networks, *Brian Yamauchi and Randall Beer*

AIC-94-005 Using a Genetic Algorithm to Search for the Representational Bias of a Collective Reinforcement Learner, *Helen G. Cobb and Peter Bock*

AIC-94-006 Simple Subpopulation Schemes, *William M. Spears*

AIC-94-007 Eucalyptus: Integrating Natural Language Input with a Graphical User Interface, *Kenneth Wauchope*

AIC-94-008 Assimilating High-Level Advice in Embedded Agents, *Devika Subramanian and Diana Gordon*

AIC-94-009 Predicting the Performance of Genetic Algorithms, *John J. Grefenstette*

AIC-94-010 Research in Advanced Software Technologies at the Naval Research Laboratory: Machine Intelligence and Formal Methods, *Randall P. Shumaker and Laura C. Davis*

AIC-94-011 Feature Selection for Case-Based Classification of Cloud Types: An Empirical Comparison, *David W. Aha and Richard L. Bankert*

AIC-94-012 Towards a Better Understanding of Memory-Based Reasoning Systems, *John Rachlin, Simon Kasif, Steven Salzberg and David W. Aha*

AIC-94-013 User's Guide to the Navigation and Collision Avoidance Task, *Diana F. Gordon, Alan C. Schultz, John J. Grefenstette, James Ballas, and Manuel A. Pérez*

AIC-94-014 An Evolutionary Approach to Learning in Robots, *Grefenstette and Alan Schultz*

AIC-94-015 Use of the User Action Notation at the Naval Reserach Human-Computer Interaction Laboratory, *Joe Chase, Deborah Hix, David Tate, and James Templeman*

AIC-94-016 Case-Based Anytime Learning, *Connie Loggia Ramsey and John J. Grefenstette*

AIC-94-017 Evolving Robot Behaviors, *Alan C. Schultz andJohn J. Grefenstette*

AIC-94-018 A Simpler Look at Consistency, *William M. Spears and Diana Gordon*

AIC-94-019 Adapting Crossover in Genetic Algorithms, *William M. Spears*

AIC-94-020 Using Markov Chains to Analyze GAFOs, *Kenneth A. De Jong, William M. Spears, and Diana Gordon*

AIC-94-021 Calibrating, Counting, Grounding, Grouping, *J. Drapkin, D. Gordon, S. Kraus, M. Miller, M. Nirkhe, and D. Perlis*

AIC-94-022 A Test of An Unsupervised Machine Learning Procedure Applied to Cloud Classification Data, *Diana Gordon, P. Tag, and R. Bakert*

AIC-94-023 Validating an Embedded Intelligent Sensor Control System, *Patrick R. Harrison and P. Ann Harrison*

AIC-94-024 Learning Recursive Relations with Randomly Selected Small Training Sets, *David W. Aha, Stephane Lapointe, Charles X. Ling, and Stan Matwin*

AIC-94-025 REPLACED BY AIC-95-043

AIC-94-026 A Comparative Evaluation of Sequential Feature Selection Algorithms, *David W. Aha and Richard L. Bankert*

AIC-94-027 Automated Identification of a Cloud Patterns in Satellite Imagery, *Richard L. Bankert and David W. Aha*

AIC-94-028 Multi-Source Data Deinterleaving With Neural Networks, *Behrooz Kamgar-Parsi, Behzad Kamgar-Parsi, and John Sciortino*

AIC-94-029 Tripod Operators for Realtime Recognition of Surface Shapes in Range Images, *Frank Pipitone*

AIC-94-030 Rapid Recognition of Elementary Surface Shapes in Cluttered Range Images Using Tripod Operators, *Frank Pipitone*

AIC-94-031 Speech and Human Language Technology at the Naval Research Laboratory, *Helen M. Gigley*

AIC-94-032 Human-Machine Dialogue for Multi-Modal Decision Support Systems, *Elaine Marsh, Kenneth Wauchope, and John O. Gurney, Jr.*

AIC-94-033 Extension of Off-Nadir View Angles for Directional Sensor Systems, *D.S. Kimes, P. Ann Harrison, and Patrick R. Harrison*

AIC-94-034 User Modeling—A Paradigm for Human-Computer Interaction, *Helen M. Gigley*

AIC-94-035 Noise Cancellation for CELP Voice encoders in an F/A-18 Noise Environment, *D. A. Heide*

AIC-94-036 Eye Tracking in Advanced Interface Design, *Robert J.K. Jacob*

AIC-94-037 Integrality and Separability of Input Devices, *Robert J.K. Jacob, Linda E. Sibert, Daniel C. McFarlane, and M. Preston Mullen, Jr.*

AIC-94-038 Brevity Code Frequencies in AEGIS Team Training Communications, *Kay Gladwell Schulze, Lisa B. Achille, Astrid Schmidt-Nielsen, and Susan L. Feldman* [CLASSIFIED DOCUMENT]

AIC-94-039 Delivery of Information Through Sound, *James. A. Ballas*

AIC-94-040 A Software Architecture for Adding New Interaction Techniques to a Command and Control Based Testbed, *James N. Templeman, Deborah Hix, and Robert J.K. Jacob*

AIC-94-041 System Effectiveness of Knowledge-Based Technology: The Relationship of User Performance and Attitudinal Measures, *Geoffrey S. Hubona and Paul H. Cheney*

AIC-94-042 Learning Natural Thresholds for Object Recognition, *Behrooz Kamgar-Parsi and Behzad Kamgar-Parsi*

AIC-94-043 Effect of Event Variations and Sound Duration on Identification of Everyday Sound, *James. A. Ballas*

AIC-94-044 A Paradigm to Assess and Evaluate Tools to Support the Software Development Process, *James. A. Ballas and Janet L. Stroup*

AIC-94-045 Genetic Algorithms: A 25 Year Perspective, *Kenneth A. De Jong*

AIC-94-046 A Natural Language Interface For Virtual Reality Systems, *Stephanie Everett, Kenneth Wauchope, and Manuel A. Pérez*

AIC-94-047 Practical Issues in the Development of an Embedded Real-Time Expert System, *Patrick R. Harrison*

AIC-94-048 An Intelligent Workbench for Analyzing Spectral Reflectance Data, *Patrick R. Harrison*

AIC-94-049 Application of AI Techniques to Infer Vegetation Characteristics from Directional Reflectance(s), *Patrick R. Harrison*

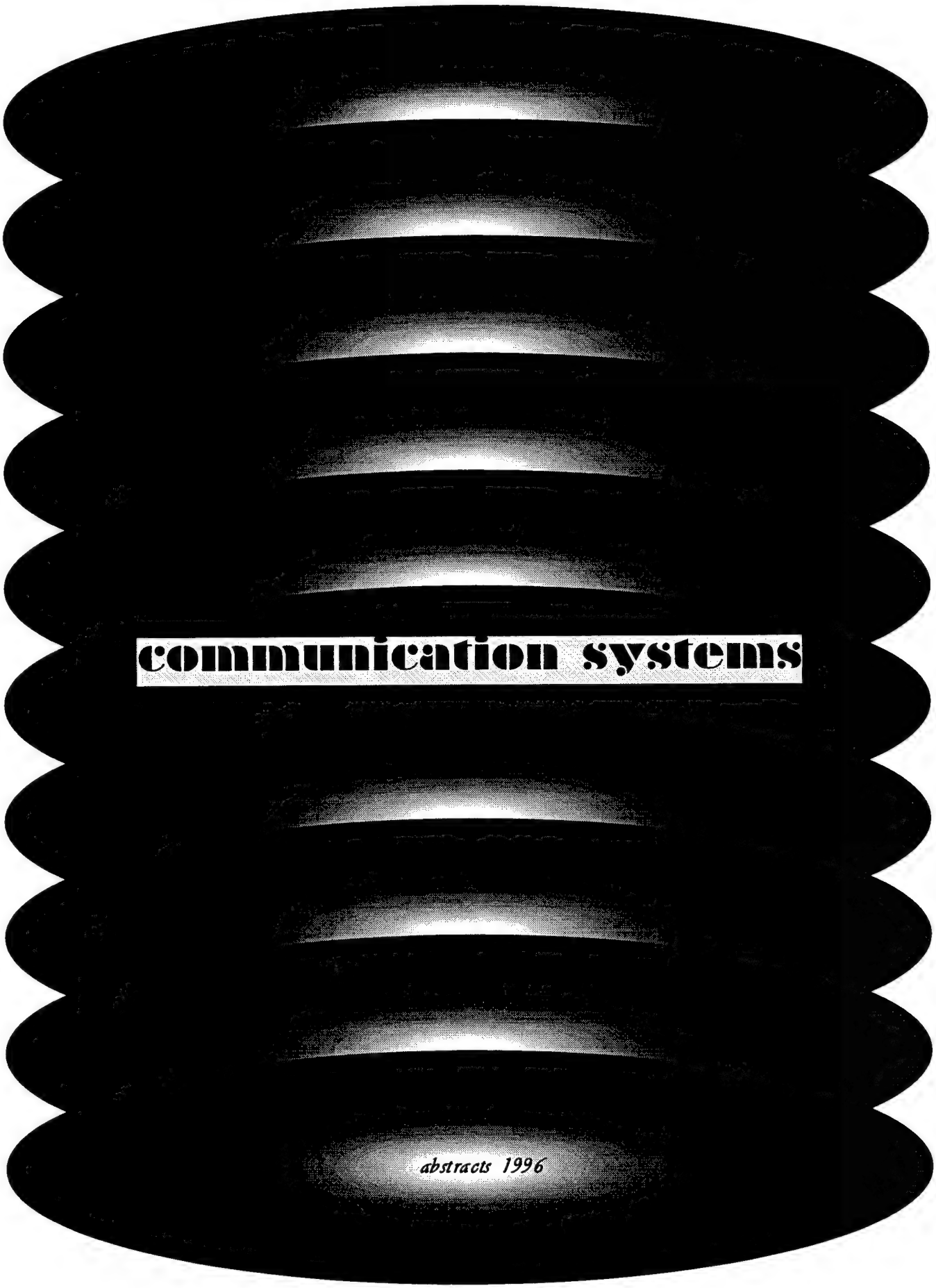
AIC-94-050 Distribution and Moments of the Weighted Sum of Uniform Random Variables, with Applications in Reducing Monte Carlo Simulations, *Behzad Kamgar-Parsi, Behrooz Kamgar-Parsi, and Menashe Brosh*

AIC-94-051 Quantization Error in Regular Grids: Triangular Pixels, *Behrooz Kamgar-Parsi and Behzad Kamgar-Parsi*

AIC-94-052 Model-based Pattern Recognition with Multilayer Neural Networks: Learning from the Eye, *Behrooz Kamgar-Parsi and Behzad Kamgar-Parsi*

AIC-94-053 A UIMS Architecture for Focus In Graphical User Interface, *Manuel A. Pérez and R.J.K. Jacob*

AIC-94-054 Modechart Toolset User's Guide, *Anne T. Rose, Manuel A. Pérez, and Paul C. Clements*


communication systems
abstracts 1996

COMMUNICATION SYSTEMS

CODE 5520

The Communication Systems (CS) Branch is the principal agent for communication system design, analysis, and engineering, with current efforts focused on strategic, tactical and special warfare areas. Emphasis is given to network design, system performance validation via computer simulation experiments, modulation and coding techniques, communication terminal design and development, advanced instrumentation techniques, and equipment development. The Branch also provides consultation and support to other components of NRL, Navy, SDIO, and DoD in the areas of secure communication equipment, systems design and development, and warfare architecture.

Title: A Simple Analysis of Average Queueing Delay in Tree Networks
Author(s): Eytan Modiano, Jeffrey E. Wieselthier, and Anthony Ephremides
E-mail Address: wieselthier@itd.nrl.navy.mil
Citation: IEEE Transactions on Information Theory, 42
Date: March 1996
Report No.: CS-96-001

Abstract

We develop an approach to the analysis of average queueing delay in a tree network of discrete-time queues with constant service time. The analysis of such systems is pertinent to packet-switched data networks with fixed-length packets. Our solution is based on considering an equivalent network, in which at each node packets in transit are given priority over exogenous arrivals. The solution to the equivalent model is easily computed, and, hence, the solution to the original model can be obtained.

Title: Efficient Evaluation and Control of DEDS via Standard Clock Simulation and Ordinal Optimization Techniques
Author(s): Craig M. Barnhart, Jeffrey E. Wieselthier, and Anthony Ephremides
E-mail Address: wieselthier@itd.nrl.navy.mil
Citation: Paper presented at INFORMS'96, Washington, DC
Date: May 1996
Report No.: CS-96-002

Abstract

In this paper we discuss the application of Standard Clock (SC) simulation and ordinal optimization techniques to examples of discrete-event dynamic systems (DEDS) such as communication networks. In SC simulation a common event sequence is used to perform a number of simultaneous simulations, thereby resulting in a significant decrease in the cost of event generation. The correlation induced by the use of the common event sequence facilitates the rapid determination of nearly optimal system control parameters by means of ordinal optimization; i.e., short simulation runs and/or easily computed approximate models provide performance rankings that are close to exact and hence facilitate the choice of a good set of control parameters.

Title: Performance and Resource Cost Comparisons for the CBT and PIM Multicast Routing Protocols in DIS Environments
Author(s): Tom Billhartz, J. Bibb Cain, Ellen Farrey-Goudreau, Doug Fieg, Steve G. Batsell, and Stuart Milner
E-mail Address: mcgregor@itd.nrl.navy.mil
Citation: Invited paper submitted to IEEE Journal on Selected Areas in Communications
Date: 1996
Report No.: CS-96-003

Abstract

Researchers have proposed the Core Based Trees (CBT) and Protocol Independent Multicasting (PIM) protocols to route multicast data on internetworks. The performance of these protocols is examined in the Distributed Interactive Simulation (DIS) environment using the OPNET network simulation tool. The simulation results provide measures of important performance metrics including end-to-end delay, network resource usage, and join time. The size of the tables containing multicast routing information and the impact of the timers introduced by the protocols are also examined. Suggestions are offered to improve PIM Sparse while retaining the ability to offer both shared tree and source-based tree routing.

Title: Constrained Optimization Methods for Admission Control and Offered Load in Communication Networks
Author(s): Craig M. Barnhart, Jeffrey E. Wieselthier, and Anthony Ephremides
E-mail Address: wieselthier@itd.nrl.navy.mil
Citation: Presented at 30th Annual Conference on Information Sciences and Systems, Princeton, N. J.
Date: March 1996
Report No.: CS-96-004

Abstract

In earlier studies [1, 2] we addressed the problem of admission control in networks that use circuit switching to support voice traffic. The goal was the determination of the admission-control policy that provided the greatest reward, which is typically the greatest total throughput or a function of throughput of the various circuit types supported by the network. In the present paper we again consider circuit-switched networks, but we shift our attention to the determination of the offered load that provides the greatest reward for a prespecified admission-control policy. Our approach is the use of Lagragian optimization techniques. We then discuss how the optimization problem can be extended to jointly optimize the admission-control policy and offered load.

Title: Data Collection Using SNMP in The DIS Environment
Author(s): R. R. Nair, Dennis N. McGregor, and Barth J. Root
E-mail Address: mcgregor@itd.nrl.navy.mil or root ?
Citation: In Proceedings of 14th Workshop on Standards for the Interoperability of Distributed Systems
Date: March 1996
Report No.: CS-96-005

Abstract

In order to collect performance data in real time from the control components of a distributed interactive simulation (DIS), a Management Information Base (MIB) was created for the principal software components to monitor internal performance values of interest and/or change internal control variables. The traditional SNMP agent on the control software host platform (SGI) was replaced by a master SNMP agent, sub-agent combination, providing every control software component with its own sub-agent. This paper decribes the SNMP

interface for the control software and the MIB structure. It also describes the performance of this data collection/monitoring/control scheme during the Synthetic Theater of War (STOW) Engineering Demonstration #1A (ED-1A) held in November, 1995, during which the control software MIB variables at all sites were queried every minute from two HP Open View Network Management Stations. In addition, the paper describes an easy and quick procedure to add SNMP interfaces to software so that they can be monitored and controlled during run-time.

Title: STOW Traffic and Related Issues
Author(s): Gam D. Nguyen and Steve G. Batsell
E-mail Address: nguyen@itd.nrl.navy.mil
Citation: Naval Laboratory Memorandum Report NRL/MR/5520-96-7842
Date: April 16, 1996
Report No.: CS-96-006

Abstract

The Distribution Interactive Simulation (DIS) program has responded to the needs of having a common, standardized environment in which a large number of simulation nodes can interact in real time with each other. An early phase of the DIS program is the Synthetic Theater of War-Europe (STOW-E) demonstration, which was conducted in November 1994.

We analyze the STOW-E traffic using sample statistical techniques and find the following: At small time scales, the LAN traffic oscillates between burstiness and smoothness, whereas the WAN traffic exhibits smoothness. However, both the LAN and the WAN traffic exhibit high burstiness on larger time scales. Therefore, the traffic shows characteristics that would be produced by Poisson-type and self-similar processes. Additionally, in comparing the STOW-E traffic with an asymptotically self-similar process, we find that it has unusually high Hurst parameter (i.e., H ~1). It is well known that time-dependent processes can yield characteristics resembling correlated components or self-similarity. A simple mathematical model for the traffic is an uncorrelated process whose parameters vary according to another asymptotically self similar process of high burstiness. Since a combination of self-similar processes results in an asymptotically self-similar process, we conjecture that future STOW traffic should behave as asymptotically modulated self-similar processes.

Title: A New Look at Double Error Correcting BCH Codes
Author(s): Paul J. Crepeau
E-mail Address: crepeau@itd.nrl.navy.mil
Citation: Presented at Conference proceedings, MILCOM '96
Date: October 1996
Report No.: CS-96-007

Abstract

We give a complete classification of the error locator polynomials that occur in the decoding of DEC BCH codes. We present a new construction showing that all quadratic error locator polynomials produced by received vectors falling in the interstitial region between decoding spheres are illegimate and have no roots.

Futhermore, we show that a small subset of received vectors in the interstitial region produce cubic error locator polynomials that are illegimate except for the correctable case of a triple error pattern with three equally spaced errors in the cyclic sense.

Title: Statistical Characteristics of DIS Traffic
Author(s): Gam D. Nguyen and Steve G. Batsell
E-mail Address: nguyen@itd.nrl.navy.mil
Citation: Conference Proceedings
Date: October 21-24, 1996
Report No.: CS-96-008

Abstract

Advanced Research Projects Agency (ARPA) has initiated the Synthetic Theater of War (STOW) program to expand the current Distributed Interactive Simulation (DIS) capability to handle larger exercises. In this paper, characterizations of the unclassified network traffic from the Synthetic Theater of War-Europe (STOW-E) demonstration are assessed in the context of self-similarity. This paper demonstrates the following from the analysis of the measured traffic. At small time scales, the LAN traffic oscillates between burstiness and smoothness, whereas the WAN traffic exhibits smoothness. However, both the LAN and the WAN traffic exhibit high burstiness on larger time scales. Therefore, the traffic shows characteristics that would be produced by Poisson-type and self-similar processes. Additionally, in comparing the STOW-E traffic with an asymptotically self-similar process, we find that it has unusually high Hurst parameter (i.e., H~1). A simple mathematical model for the traffic is an uncorrelated process whose parameters vary according to another asymptotically self similar process of high burstiness. Since a combination of self-similar processes results in an asymptotically self-similar process, we conjecture that future STOW traffic should behave as asymptotically modulated self-similar processes.

Title: New Reliable Error-Detection Codes and Their Fast Implementations
Author(s): Gam D. Nguyen
E-mail Address: nguyen@itd.nrl.navy.mil
Citation: Conference Proceedings
Date: October 21-24, 1996
Report No.: CS-96-009

Abstract

This paper discusses a technique for constructing a new class of reliable codes that have efficient software and hardware implementations as well as flexible design parameters such as minimum distances, codeword lengths, and error-detecting capability. The newly constructed codes possess two key design parameters that specify length and burst-error-detecting capability. In particular, for smaller values of overhead (e.g., 8 or 16 bits), the codes can have very long codeword lengths for higher rate; whereas for larger overhead (e.g., 32 bits or more) the optimal lengths (which can be impracticably large) are not needed; however, the codes can be tailored to yield higher burst-error detection.

Furthermore, in contrast to the slow bitwise procedure of the cyclical redundancy codes (CRCs), the new codes are bytewise-oriented; hence, they are more easily implemented in modern computers and networks.

Title: Efficient Evaluation and Control of DEDS Via Standard Clock Simulation and Ordinal Optimization Techniques
Author(s): Craig M. Barnhart, Jeffrey E. Wieselthier, and Anthony Ephremides
E-mail Address: wieselthier@itd.nrl.navy.mil
Citation: Conference Proceedings and Oral Presentation
Date: May 5-8, 1996
Report No.: CS-96-010

Abstract

In this paper we discuss the application of Standard Clock (SC) simulation and ordinal optimization techniques to examples of discrete-event dynamic systems (DEDS) such as communication networks. In SC simulation a common event sequence is used to perform a number of simultaneous simulations, thereby resulting in a significant decrease in the cost of event generation. The correlation induced by the use of the common event sequence facilitates the rapid determination of nearly optimal system control parameters by means of ordinal optimization; i.e., short simulation runs and/or easily computed approximate models provide performance rankings that are close to exact and hence facilitate the choice of a good set of control parameters.

Title: A Fast Method for Combining/Generating Synthetic Traffic Traces Exhibiting Short- and Long-Range Dependence
Author(s): Gam D. Nguyen
E-mail Address: nguyen@itd.nrl.navy.mil
Citation: International Conference on Computer Communications and Networks, October 16-19, 1996
Date: October 16-19, 1996
Report No.: CS-96-011

Abstract

We consider a heuristic approach for combining short traffic traces of various degrees of self-similarity to produce a longer trace that has the following desirable properties. The mixed trace is capable of modeling computer networking traffic that exhibits both short- and long-range dependence in a unified model. Synthetic traces of self-similar characteristics can be generated quickly due to the simplicity of our method, which is faster than the traditional approach of generating/approximating traffic traces from nothing.

Title: A Polynomial Construction of Perfect Codes
Author(s): Gam D. Nguyen
E-mail Address: nguyen@itd.nrl.navy.mil
Citation: Submitted to International Journal of Computer Mathematics
Date: May 1996
Report No.: CS-96-012

Abstract

Starting with a single-error-correcting extended perfect binary systematic code of length S, one can construct a single-error-correcting extended perfect binary systematic code of length $S2^S$ by polynomial manipulations.

Title: Multiple-Ring Architecture and its FDDI Applications
Author(s): Gam D. Nguyen
E-mail Address: nguyen@itd.nrl.navy.mil
Citation: IEEE Military Communications Conference, McLean, VA, October 21-24, 1996
Date: October 21-24, 1996
Report No.: CS-96-013

Abstract

This paper discusses a networking concept, which we refer to as Multiple-Ring Architecture (MRA). For reliability applications of the Fiber Distributed Data Interface network, MRA is an attractive alternative to the popular dual homing architecture for the following reason. Unlike the requirement of several reliable concentrators needed in the dual homing architecture, the MRA only requires several routing interfaces at each backbone node (i.e., at each router node); different fiber cables and networks share the same set of routers, creating a set of highly fault tolerant networks of low overall cost and complexity.

Title: Conversion of MIL-T-28800 to a Performance Specification
Author(s): Joseph A. Molnar
E-mail Address: molnar@itd.nrl.navy.mil
Citation: Conference Proceedings
Date: September 1996
Report No.: CS-96-014

Abstract

MIL-T-28800 is a specification for the environmental requirements of test equipment. Authorization was obtained to convert MIL-T-28800 to a performance specification and reissue it as MIL-PRF-28800F to conform with the guidance provided for Acquisition Reform. The conversion was completed in June 1996. Major aspects of the conversion are discussed including the replacement of Military specification references with commercial and international standards references.

Title: A Problem of Constrained Optimization for Bandwidth Allocation in High-Speed and Wireless Communication Networks
Author(s): Jeffrey E. Wieselthier, Craig M. Barnhart, and Anthony Ephremides
E-mail Address: wieselthier@itd.nrl.navy.mil
Citation: Invited paper presented at the 35th IEEE Conference on Decision and Control, Kobe, Japan, December 11-13, 1996
Date: December 11-13, 1996
Report No.: CS-96-015

Abstract

In this paper we consider this aspect of network control. We do not focus on a detailed description of network traffic (such as ATM, which supports a variety of traffic types including Constant Bit Rate, etc.) but, rather, look at a more generic formulation, which permits a solvable formulation of the associated optimization problem. Specifically, we assume a circuit-switched, fixed-route network with independent Poisson arrivals of session-establishment requests over each of the fixed routes. The objective is to decide on an optimal admission-control policy that maximizes throughput, subject to the constraint that blocking probability on every route stays below a given level.

Title: A Recommended Error Control Architecture and Issues for ATM Networks With Wireless Links
Author(s): J. Bibb Cain and Dennis N. McGregor,
E-mail Address: mcgregor@itd.nrl.navy.mil
Citation: Submitted to the Journal Selected Areas in Communications
Date: 1996
Report No.: CS-96-016

Abstract

This paper provides performance results through analysis and simulation for key error control problems encountered in using wireless links to transport ATM cells. Problems considered include the Forward Error Correction (FEC) and interleaving at the physical layer, the impact of wireless links on the ATM cell Header Error Control (HEC) and Cell Delineation (CD) functions, the application of data link ARQ for traffic requiring reliable transport, and the impact of the choice of end-to-end ARQ protocol for reliable service. We conclude that it is very important to make the physical layer as SONET-like as possible through the use of powerful FEC, interleaving, and ARQ. These additional error control measures are especially necessary for disturbed channels because of the degrading effects of the channel on higher-layer functions. A recommended error control architecture is given with tradeoffs.

Title: Optimization of Admission Control in Wireless Networks
Author(s): Jeffrey E. Wieselthier, Craig M. Barnhart, Anthony Ephremides, and Gam D. Nguyen
E-mail Address: wieselthier@itd.nrl.navy.mil or nguyen@itd.nrl.navy.mil
Citation: Workshop on New Techniques for Radio Communications and Wireless Networks, , San Diego, CA, September 10-12, 1996
Date: September 10-12, 1996
Report No.: CS-96-017

Abstract

We consider integrated voice/data multihop wireless networks, in which circuit switching is used for voice traffic and packet switching is used for data traffic. In such systems it may be advantageous to block a newly arriving voice call even though resources are currently available, because the acceptance of a particular call now may result in the blockage of several other future calls (or perhaps a call

of higher precedence) that could otherwise have been accepted. Alternatively, in integrated networks the acceptance of too many voice calls may result in the unavailability of sufficient network resources to support data traffic.

Title: Mobile Internetworking Design Issues for Littoral and Expeditionary Warfare
Author(s): Dennis N. McGregor, Edwin L. Althouse, and Donald F. Gingras
E-mail Address: mcgregor@itd.nrl.navy.mil or althouse@itd.nrl.navy.mil
Citation: Workshop on New Techniques for Radio Communications and Wireless Networks, San Diego, CA, September 10-12, 1996
Date: September 1996
Report No.: CS-96-018

Abstract

Joint forces engaging in littoral and expeditionary warfare operations currently do not have the timely and seamless capability to transfer information among widely dispersed mobile groups. A need exists for OTH information distribution during the early phases of expeditionary warfare when the littoral activities are very dynamic. During this period, high-bandwidth communication trunk lines are generally not available to many of the participating entities. Activities include Mine Countermeasures (MCM) operations of mine sweeping and lane clearing, Naval Surface Fire Support (NSFS) to hold off resistance from the shore, submarine acoustical surveillance, airborne surveillance and attack, and amphibious assault. The operational success of these missions is greatly enhanced if they are coordinated with each other. Such a capability requires a responsive communications system that provides wireless network connectivity among the warfighting domains, including those of the CLF, CATF, CJTF, MCM, NSFS, and the surveillance product. Joint Service personnel must have the capability to establish and coordinate data/voice communication rapidly in any given area.

Title: An Error Control Architecture for ATM Networks with Wireless Links
Author(s): Joseph B. Cain and Dennis N. McGregor
E-mail Address: mcgregor@itd.nrl.navy.mil
Citation: Workshop on New Techniques for Radio Communications and Wireless Networks, San Diego, CA, September 10-12, 1996
Date: September 10-12, 1996
Report No.: CS-96-019

Abstract

The purpose of this presentation is to investigate error control issues encountered in using ATM over wireless data links. These results will show that ATM, the basic transport mechanism for BISDN, can be made to perform satisfactorily over wireless data links if certain error control measures are used to insure that RF link characteristics do not impair ATM operation. A major problem that must be considered is that the protocol layers in an ATM network were designed with the assumption of a very high quality data link. This is true not only of ATM, but also of TCP which is often used above ATM to provide reliable delivery. In fact, one of the reasons that ATM can be switched at very high

speeds is due to the simplification of the protocol via eliminating features such as link level error control (on the assumption of a near error-free link). Thus, the protocol stack consists of a number of protocols that were not designed with the objective of working together optimally with low quality links. In fact, the opposite is true. These protocols, when used together over low quality links, can behave quite poorly. The impact of link characteristics on a variety of ATM functions and on overall system performance are presented. We will present an error control architecture for improving the quality of wireless links to make them closer to fiber link quality. The architecture will use Forward Error Correction (FEC), interleaving, and data link layer ARQ for traffic requiring reliable delivery. The optimization of the error control mechanisms and parameters within this architecture will be influenced by the type of wireless link and its intended usage.

Title: Data/Voice Integration Advanced Technology Demonstration
Author(s): Edwin L. Althouse
E-mail Address: althouse@itd.nrl.navy.mil
Citation: Oral Presentation at NRL to Diverse Outside Audience and Publication on World-Wide-Web
Date: November 1996
Report No.: CS-96-020

Abstract

While the ability to support integrated services, such as data, voice, and video has become common-place in today's computer networks, military tactical networks are still primarily single purpose and support either data-only or voice-only services. For modern warfare, tactical networks will be required to become an extension to shipboard local/wide-area networks and high-speed terrestrial and satellite information-supply lines. The technological obstacles are that (a) integrated services are difficult to achieve on low-data-rate tactical networks and links and (b) there are great technical obstacles and few funded programs to increase data rates on tactical networks.

Title: Summary and Applicability of Analog Fault Detection/Isolation Techniques
Author(s): Joseph A. Molnar
E-mail Address: molnar@itd.nrl.navy.mil
Citation: Internal Report
Date: 1996
Report No.: CS-96-021

Abstract

A survey of common analog fault diagnostic techniques is provided. The focus is on providing information to facilitate the use of viable techniques suited for a problem definition. The level of understanding of the analog system is correlated with the type of techniques best suited for the diagnostic system. Reviewed are techniques from Control Theory, Probability Theory, Computational Expert Systems, and Computational Artificial Intelligence. The Control Theory techniques are suited best for system diagnostic problems where the system model is accurately understood. Techniques that employ Probability ory are valuable for addressing uncertainty that arises in diagnostics of

systems affected by noise. Computational Expert Systems address the problem of diagnostics by creating a data structure to represent the diagnostic process or system relationship representation. The technique can be used to great advantage in situations where the diagnostic process is accurately understood. Computation Artificial Intelligence techniques are presented as being best suited for systems where little reliable knowledge is known. The analysis does not preclude the use of any technique, but rather addresses efficiency of application.

Title: W-Band Synthesized Signal Generator Using Fundamental Voltage Controlled Oscillators
Author(s): Joseph A. Molnar and Richard Zborofsky
E-mail Address: molnar@itd.nrl.nvy.mil
Citation: Internal Report
Date: 1996
Report No.: CS-96-022

Abstract

The architecture and implementation of a W-Band signal generator are described. The architecture presented, highlights the developmental areas of the signal source, frequency control, output control, and modulation. Voltage controlled oscillators (VCOs) were developed to provide frequency agility, to enhance the visability of frequency modulation (FM) characteristics, and to improve weight and power management requirements. Frequency control and phase coherence were achieved through the exploitation of digital phase lock loop (PLL) techniques. PIN diode attenuators that were developed cover the entire W-Band and provide the capacity for output level control. Additionally, the attenuators provide the capacity for amplitude modulation (AM) and pulse modulation (PM) because of the attenuation flatness (<5dB), large dynamic range (>40dB), and modulation bandwidth. A prototype has been developed to demonstrate the feasibility. The final implementation will be integrated into a C-sized VXI module chassis.

1995 PUBLICATIONS

CS-95-001 Admission-Control Policies for Multihop Wireless Networks, *Craig M. Barnhart, Jeffrey E. Wieselthier, and Anthony Ephremides*

CS-95-002 Standard Clock Simulation and Ordinal Optimization Applied to Admission Control in Integrated Communication Networks, *J.E. Wieselthier, C.M. Barnhart and Anthony Ephremides*

CS-95-003 Multi-Access Strategies for an Integrated Voice/Data CDMA Packet Radio Network, *Mohsen Soroushnejad and Evaggelos Geraniotis*

CS-95-004 Ordinal Optimization of Admission Control in Wireless Multihop Integrated Networks via Standard Clock Simulation, *Jeffrey E. Wieselthier, Craig M. Barnhart, and A. Ephremides*

CS-95-005 Voice Management and Multiplexing Protocols Developed for the Data and Voice Integration Advanced Technology Demonstration, *James P. Hauser*

CS-95-006 Real-Time Network Packet Voice Support in the Data Voice Integration Advanced Technology Demonstration, *Joseph P. Macker*

CS-95-007 Quality Assurance, Alignment, and Test Procedure for the MD-1310/U Modulator, *J.A. Molnar and E.R. Farren*

CS-95-008 Novel Techniques for the Analysis of Wireless Integrated Voice/Data Networks, *Jeffrey E. Wieselthier, Craig M. Barnhart, and Anthony Ephremides*

CS-95-009 Integrated Computer Aided Design Practices as Demonstrated on A Fin-Line Device, *Joseph A. Molnar*

CS-95-010 MD-1310/U VLF/LF Modulator Functionality and Performance Test Report, *T.H. Gattis*

CS-95-011 Adding Training Capability to COTS Network Management Software, *Radhakrishnan R. Nair and Dennis N. McGregor*

CS-95-012 Tactical Radio Frequency Requirements for Next Generation Internet Protocols, *Robert B. Adamson*

CS-95-013 Coding and Synchronization Analysis of the NILE UHF Fixed-Frequency Waveform, *Paul J. Crepeau and John C. McCanless*

CS-95-014 On Burst-Error Detecting Capability of Weighted Sum Codes, *Gam D. Nguyen*

CS-95-016 IVOX The Interactive VOice eXchange Application, *Joseph P. Macker and R. Brian Adamson*

CS-95-017 A New Family of Reliable Error Detection Codes Having Low Complexity, *Gam D. Nguyen*

CS-95-018 A Neural Network Approach to Solving the Link Activation Problem in Multihop Radio Networks, *C. M. Barnhart, J. E. Wieselthier, and A. Ephremides*

CS-95-019 Platform-Related Limitations to Efficiency in Standard Clock Simulation on Sequential Machines, *C. M. Barnhart, J. E. Wieselthier, and A. Ephremides*

CS-95-021 Noise Issues in Optical Linear Algebra Processor Design, *S. G. Batsell, J. F. Walkup, and T. F. Krile*

CS-95-022 The Implications of a Distributed Computing Paradigm on Multicast Routing, *S. G. Batsell and J. E. Klinker*

CS-95-025 MCA Protocols and Algorithms, *K. Burrows, D. Nguyen, E. Rubin, E. Smythe, and W. Thoet*

CS-95-026 Performance Analysis of ATM Networks With Wireless Links, *J. B. Cain*

CS-95-027 Key Performance Issues for ATM Networks with Wireless Links, *J. B. Cain and D. N. McGregor*

CS-95-028 Parallel Sample Path Generation for Discrete Event Systems and the Traffic Smoothing Problem, *C. G. Cassandras and J. Pan*

CS-95-029 Scheduling Policies Using Marked/Phantom Slot Algorithms, *C. G. Cassandras and V. Julka*

CS-95-030 A Reservation Based Multicast (RBM) Routing Protocol for Mobile Networks: Initial Route Construction Phase, *M.S. Corson and S. G. Batsell*

CS-95-031 A Reservation Based Multicast (RBM) Routing Protocol for Model Networks: Initial Routing Construction, *M. S. Corson and S. G. Batsell*

CS-95-032 Admission Control and Bandwidth Allocation in High-Speed Networks as a System Theory Problem, *A. Ephremides, J. E. Wieselthier, and C. M. Barnhart*

CS-95-033 A Multiple-Access Scheme for Voice/Data Integration in Hybrid Satellite/Terrestrial Packet Radio Networks, *E. Geraniotis, M. Soroushnejad, and W. B. Yang*

CS-95-034 Adding SNMP Interface to Applications, *R. R. Nair*

CS-95-035 Design of SNMP Interface for Application Control Software, *R. R. Nair*

CS-95-036 Multi-Access Strategies for an Integrated Voice/Data CDMA Packet Radio Network, *M. Soroushnejad and E. Geraniotis*

CS-95-037 "A Mini-Product-Form-Based Solution to Data-Delay Evaluation in Wireless Integrated Voice Data Networks, *J. E. Wieselthier, C. M. Barnhart, and A. Ephremides*

CS-95-038 Fixed- and Movable-Boundary Channel-Access Schemes for Integrated Voice/Data Networks, *J. E. Wieselthier and A. Ephremides*

CS-95-039 Data-Delay Evaluation in Integrated Wireless Networks based on Local Product-Form Solutions for Voice Occupancy, *J. E. Wieselthier, C. M. Barnhart, and A. Ephremides*

CS-95-040 Integrated Services in Tactical Communication Systems, *E. L. Althouse, J. P. Macker, J. P. Hauser, and D. J. Baker*

CS-95-041 Tri-Service Requirements and Growth Capabilities Report, *J. B. Cain and K. Kirk*

CS-95-042 Communication Systems Network Interoperability, *Robert B. Adamson*

1994 PUBLICATIONS

CS-94-001 Ordinal Optimization by Means of Standard Clock Simulation and Crude Analytical Models, *Craig M. Barnhart, Jeffrey E. Wieselthier, and Anthony Ephremides*

CS-94-002 Reed-Solomon Coding Performance with Errors and Erasures Decoding on a Rayleigh Fading Channel, *Paul J. Crepeau and Karen W. Halford*

CS-94-003 Integrated Computer Aided Design Practices As Demonstrated On a Fin-Line Device, *J. A. Molnar*

CS-94-004 Ordinal Optimization of Admission Control in Wireless Multihop Integrated Networks via Standard Clock Simulation, *Jeffrey E. Wieselthier and Craig M. Barnhart*

CS-94-005 A New Look at Double Error Correcting BCH Codes, *P. J. Crepeau*

CS-94-006 Discrete-Event-Dynamic-System-Based Approaches for Control in Integrated Voice/Data Multihop Radio Networks, *J. E. Wieselthier, C. G. Cassandras, and Vibhor Julka*

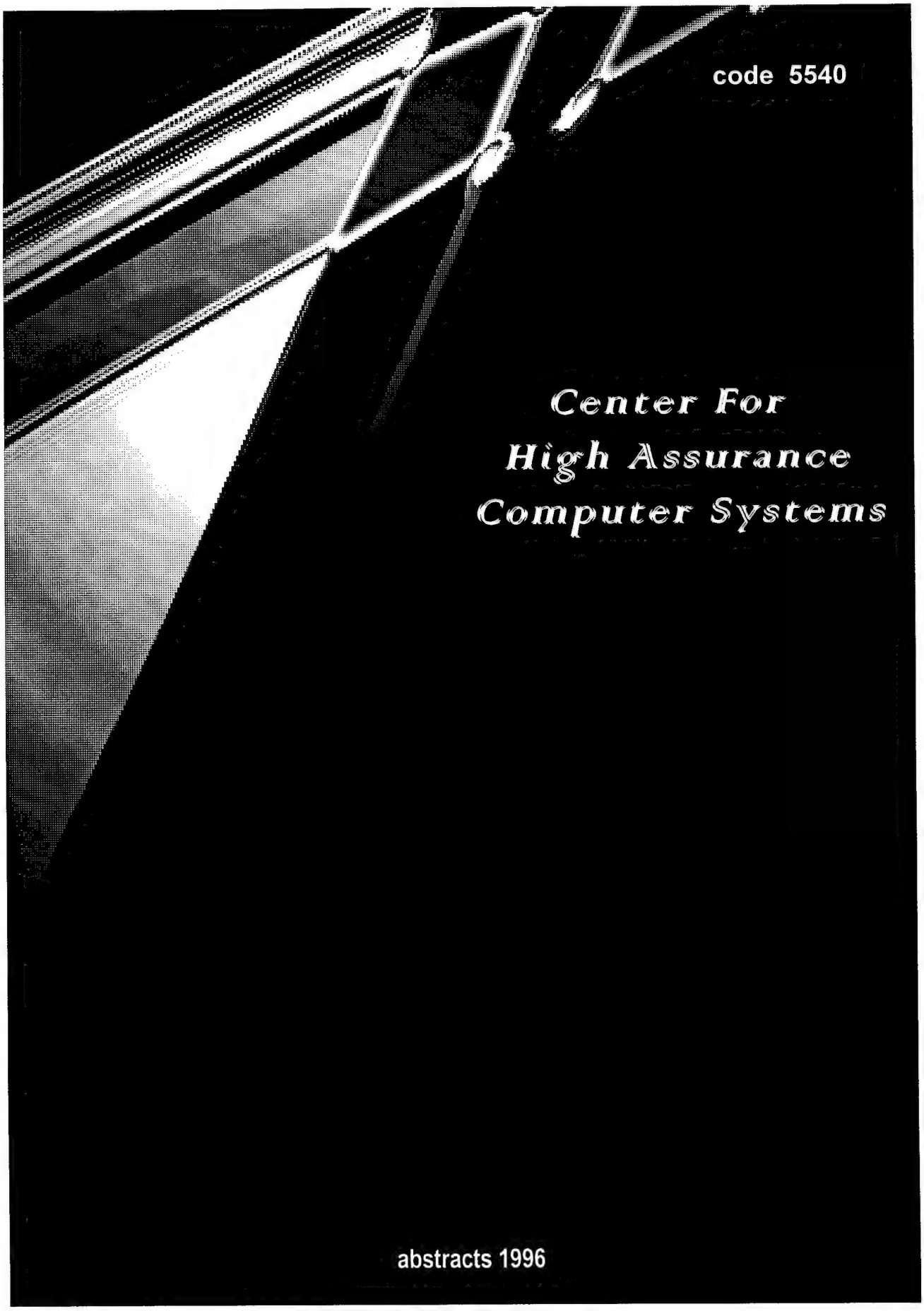
CS-94-007 Book Review of "The Collected Papers of Claude Shannon", *P.J. Crepeau*

CS-94-008 Schemes for Reliable Message Delivery in NATO Improved Link Eleven (NILE) Networks, *M.J. Chung and D.G. Kallgren*

CS-94-009 A Mini-Product-Form-Based Solution to Data-Delay Evaluation in Wireless Integrated Voice/Data Networks, *J.E. Wieselthier, C.M. Barnhart and A. Ephremides*

CS-94-010 Functional, Electrical, and Mechanical Description of the W-Band Noise Measurement System and the NRL W-Band VXI Module, *J.A. Molnar and T.V. Mai*

CS-94-011 An Integrated Knowledge Acquisition and Database Management System, *C.B. Barclay and J.A. Molnar*


code 5540
Center For
High Assurance
Computer Systems
abstracts 1996

CENTER FOR HIGH ASSURANCE COMPUTER SYSTEMS

CODE 5540

The Center for High Assurance Computer Systems (CHACS) performs research and develops technology in areas supporting military requirements for communication security (COMSEC) and computer security (COMPUSEC). Emphasis is given to the development of concepts, architectures, analysis techniques and methodology that exploit appropriately the opportunities available through systematic consideration of the total security problem and its impact on communication and computer systems. The Center provides leadership and is the Navy's lead laboratory for research and development of COMPUSEC technology and evaluation techniques. Areas of activity include development of information security devices, subsystems and system technology through the conceptual, analysis and experimentation, and proof-of-concept phases. The Center works closely with Navy system developers and with the National Security Agency.

Title: Mechanical Verification of Timed Automata: A Case Study
Author(s): Myla M. Archer and Constance L. Heitmeyer
E-mail Address: archer@itd.nrl.navy.mil or heitmeyer@itd.nrl.navy.mil
Citation: Proceedings of the 1996 Real-Time Technology and Applications Symposium, Boston, MA, pp192-203
Date: June 10-13, 1996
Report No.: CHACS-96-001

Abstract

This paper reports the results of a case study on the feasibility of developing and applying mechanical methods, based on the proof system PVS, to prove propositions about real-time systems specified in the Lynch-Vaandrager timed automata model. In using automated provers to prove propositions about systems described by a specific mathematical model, both the proofs and the proof rocess can be simplified by exploiting the special properties of the mathematical model. This paper presents the PVS specification of three theories that underlie the timed automata model, a template for specifying timed automata models in PVS and an example of its instantiation, and both hand proofs and the corresponding PVS proofs of two propositions. It concludes with a discussion of our experience in applying PVS to specify and reason about real-time systems modeled as timed automata.

Title: Implementation of IPv6 in 4.4 BSD
Author(s): Randall J. Atkinson, Daniel L. McDonald, Bao G. Phan, Craig W. Metz, and Kenneth C. Chin
E-mail Address: phan@itd.nrl.navy.mil
Citation: Proceedings of the 1996 Technical Conference, USENIX Association, San Diego, CA, pp113-125
Date: January 1996
Report No.: CHACS-96-002

Abstract

The widespread availability of the TCP/IP protocols in early versions of BSD UNIX fostered the current widespread use of those protocols in commercial products. Recently the Internet Engineering Task Force (IETF) has designed version 6 of the Internet Protocol (IPv6). IPv6 has some similarities with IPv4, but it also has many differences, most notably in address size. This paper describes our experience creating a freely distributable implementation of IPv6 inside 4.4 BSD, with focus on the areas that have changed between the IPv4 and IPv6 implementations.

Title: Several Secure Store and Forward Devices
Author(s): David M. Goldschlag
E-mail Address: goldschlag@itd.nrl.navy.mil
Citation: Proceedings of the Third ACM Conference on Computer and Communications Security, New Delhi, India, pp129-137
Date: March 1996
Report No.: CHACS-96-003

Abstract

DoD system high enclaves are often isolated from systems at other security levels because the usual connectors (guards) are expensive to procure, integrate, accredit, and operate, and usually require a human in the middle to review the data flow, independent of direction. This isolation reduces the effectiveness of information systems. The secure store and forward devices described in this paper can be used to solve an important (yet tractable) half of the problem: moving data from LOW to HIGH without a human in the middle. These devices were expressly designed to be easy to accredit. Security critical function is both minimized and separated from non-security critical function to reduce the need for trusted components. A prototype implementation of one of these store and forward devices is described as well.

Title: Hiding Routing Information
Author(s): David M. Goldschlag, Michael G. Reed, and Paul F. Syverson
E-mail Address: goldschlag@itd.nrl.navy.mil or reed@itd.nrl.navy.mil or syverson@itd.nrl.navy.mil
Citation: In Information Hiding, Lecture Notes in Computer Science, Springer-Verlag, v1174, edited by Ross Anderson, pp137-150
Date: June 1996
Report No: CHACS-96-004

Abstract

This paper describes an architecture, *Onion Routing*, that limits a network's vulnerability to traffic analysis. The architecture improves upon anonymous re-mailers in two ways: It applies to more than just mail; and it provides better hiding (both location and identity). Specifically, it provides real-time bi-directional anonymous communication for any protocol that can be adapted to use a proxy service. Also, the architecture provides for bi-directional communication even though no-one but the initiator's proxy server knows anything but previous and next hops in the communication chain. This implies that neither the respondent nor his proxy server nor any external observor need know the identity of the initiator or his proxy server. A prototype of *Onion Routing* that works with HTTP (World Wide Web) requests will be implemented by May.

Title: Requirements Specifications for Hybrid Systems
Author(s): Constance L. Heitmeyer
E-mail Address: heitmeyer@itd.nrl.navy.mil
Citation: Proceedings, Hybrid Systems Workshop III, Lecture Notes in Computer Science, Springer-Verlag, edited by R. Alur, T. Henzinger, and E. Sontag, pp304-314
Date: 1996
Report No.: CHACS-96-005

Abstract

This paper presents a formal framework for representing and reasoning about the requirements of hybrid computer systems. By a hybrid computer system, we mean a computer system whose environment includes both continuous and

discrete entities. As background, the paper briefly reviews an abstract model for specifying system and software requirements, called the Four Variable Model, and a related requirements method, called SCR (Software Cost Reduction). The paper then introduces a special discrete version of the Four Variable Model, called the SCR requirements model, and suggests how the SCR model can be extended to specify and to reason about hybrid systems. Examples of how the SCR model can be used to specify a system's timing and accuracy requirements are given.

Title: Automated Consistency Checking of Requirements Specifications
Author(s): Constance L. Heitmeyer, Ralph D. Jeffords, and Bruce G. Labaw
E-mail Address: heitmeyer@itd.nrl.navy.mil or jeffords@itd.nrl.navy.mil
Citation: ACM Transactions on Software Engineering and Methodology, v5, n3, July 1996, pp231-261.
Date: July 1996
Report No.: CHACS-96-006

Abstract

This paper describes a formal analysis technique, called consistency checking, for automatic detection of errors, such as type errors, non determinism, missing cases, and circular definitions, in requirements specifications. The technique is designed to analyze requirements specifications expressed in the SCR (Software Cost Reduction) tabular notation. As background, the SCR approach to specifying requirements is reviewed. To provide a formal semantics for the SCR notation and a foundation for consistency checking, a formal requirements model is introduced; the model represents a software system as a finite state automaton, which produces externally visible outputs in response to changes in monitored environmental quantities. Results are presented of two experiments which evaluated the utility and scalability of our technique for consistency checking in a real-world avionics application. The role of consistency checking during the requirements phase of software development is discussed.

Title: A Network Pump
Author(s): Myong H. Kang, Ira S. Moskowitz, and Daniel C. Lee
E-mail Address: mkang@itd.nrl.navy.mil or moskowitz@itd.nrl.navy.mil
Citation: IEEE Transactions on Software Engineering, v22, n5, May 1996, pp329-338
Date: May 1996
Report No.: CHACS-96-007

Abstract

A designer of reliable multi-level secure (MLS) networks must consider covert channels and denial of service attacks in addition to traditional network performance measures such as throughput, fairness, and reliability. In this paper we show how to extend the NRL data Pump to a certain MLS network architecture in order to balance the requirements of congestion control, fairness, good performance, and reliability against those of minimal threats from covert channels and denial of service attacks. We back up our claims with simulation results.

Title: Towards a Model of Storage Jamming
Author(s): John P. McDermott and David Goldschlag
E-mail Address: mcdermot@itd.nrl.navy.mil or goldschlag@itd.nrl.navy.mil
Citation: Proceedings of the Ninth Computer Security Foundations Workshop, Kenmare, Ireland, pp176-185.
Date: June 1996
Report No.: CHACS-96-008

Abstract

Storage jamming can degrade real-world activities that share stored data. Storage jamming is not prevented by access controls or cryptographic techniques. Verification to rule out storage jamming logic is impractical for shrink-wrapped software or low-cost custom applications. Detection mechanisms do offer more promise. In this paper, we model storage jamming and a detection mechanism, using Unity logic. We find that Unity logic, in conjunction with some high-level operators, models storage jamming in a natural way and allows us to reason about susceptibility, rate of jamming, and impact on persistent values.

Title: A Socket-based Key Management API for BSD UNIX
Author(s): Daniel L. McDonald, Bao G. Phan, and Randall J. Atkinson
E-mail Address: phan@itd.nrl.navy.mil
Citation: Proceedings of INET'96 Conference, Internet Society, Reston,VA
Date: June 1996
Report No.: CHACS-96-009

Abstract

This paper presents an Application Programming Interface (API) which, in combination with interfaces presented to a networking protocol implementation, provides a set of abstractions allowing different session key management schemes to be securely built outside the operating system kernel. This permits a more modular key management implementation, which in turn facilitates a high assurance implementation of a key management protocol and permits system administrators to change or add key management modules more easily.

Title: Language Generation and Verification in the NRL Protocol Analyzer
Author(s): Catherine A. Meadows
E-mail Address: meadows@itd.nrl.navy.mil
Citation: Proceedings of the 9th Computer Security Foundations Workshop, IEEE Computer Society Press. pp48-61
Date: June 1996
Report No.: CHACS-96-010

Abstract

The NRL Protocol Analyzer is a tool for proving security properties of cryptographic protocols, and for finding flaws if they exist. It is used by having the user first prove a number of lemmas stating that infinite classes of states are

unreachable, and then performing an exhaustive search on the remaining state space. One main source of difficulty in using the tool is in generating the lemmas that are to be proved. In this paper we show how we have made the task easier by automating the generation of lemmas involving the use of formal languages.

Title: Analyzing the Needham-Schroeder Public Key Protocol: A Comparison of Two Approaches
Author(s): Catherine A. Meadows
E-mail Address: meadows@itd.nrl.navy.mil
Citation: Proceedings of ESORICS, Springer Verlag, pp. 351-364
Date: September 1996
Report No.: CHACS-96-011

Abstract

In this paper we contrast the use of the NRL Protocol Analyzer and Gavin Lowe's use of the model checker to analyze the Needham-Schroeder public key protocol. This is used as a basis to compare and contrast the two systems and to point out possible future directions for research.

Title: An Implementation of the Pump: The Event Driven Pump
Author(s): Bruce Montrose and Myong H. Kang
E-mail Address: montrose@itd.nrl.navy.mil or mkang@itd.nrl.navy.mil
Citation: Naval Research Laboratory Memorandum Report NRL/MR/5540--96-7850
Date: May 1996
Report No.: CHACS-96-012

Abstract

As computer systems become more open and interconnected, the need for reliable and secure communication also increases. In this report, we discuss a communication device, the NRL Pump, and introduce an implementation of the Pump: the Event Driven Pump that balances the requirements of reliability and security. The Pump provides acknowledgments (Acks) to the message source to insure reliability. These Acks are also used for flow control to inhibit the Pump's buffer from becoming or staying full. This is desirable because once the buffer is filled there exists a huge covert communication channel. We have prepared this report for system designers and programmers who want to understand the basic structure of the event-driven Pump. We also hope this report is helpful to the people who will maintain the Pump code. In this report, we assume that the reader is familiar with the material presented in previous Pump papers.

Title: The RS-232 Character Repeater Refinement and Assurance Argument
Author(s): Andrew P. Moore and Charles N. Payne Jr.
E-mail Address: moore@itd.nrl.navy.mil
Citation: Naval Research Laboratory Memorandum Report NRL/MR/5540--96-7872
Date: July 1996
Report No.: CHACS-96-013

Abstract

Past experience in system security certification indicates the need for developers of high assurance systems to coherently integrate the evidence that their system satisfies its critical requirements. This document describes a method based on literate programming techniques to help developers present the evidence they gather in a manner that facilitates the certification effort. We demonstrate this method through the implementation and verification of a small but non-trivial, security-relevant example, an RS-232 character repeater. By addressing many of the important issues in system design, we expect that this example will provide a model for developing assurance arguments for full-scale composite systems with corresponding gains in the expediency of the system certification process.

Title: Increasing Assurance with Literate Programming Techniques
Author(s): Andrew P. Moore and Charles N. Payne Jr.
E-mail Address: moore@itd.nrl.navy.mil
Citation: Proceedings of the 11th Annual Conference on Computer Assurance, pp 187-198
Date: June 1996
Report No.: CHACS-96-014

Abstract

The assurance argument that a trusted system satisfies its information security requirements must be convincing, because the argument supports the accreditation decision to allow the computer to process classified information in an operational environment. Assurance is achieved through understanding, but some evidence that supports the assurance argument can be difficult to understand. This paper describes a novel application of a technique, called literate programming, that significantly improves the readability of the assurance argument while maintaining its consistency with formal specifications that are input to specification and verification systems. We describe an application of this technique to a simple example and discuss the lessons learned from this effort.

Title: An Analysis of the Timed Z-Channel
Author(s): Ira S. Moskowitz, Steven J., and Myong H. Kang
E-mail Address: moskowitz@itd.nrl.navy.mil or mkang@itd.nrl.navy.mil
Citation: Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, pp2-11
Date: May 6-8, 1996
Report No.: CHACS-96-015

Abstract

Our timed Z-channel (a general case of the Z-channel) appears as the basis for a large class of covert channels. Golomb analyzed the Z-channel, a memoryless channel with two input symbols and two output symbols, where one of the input symbols is transmitted with noise while the other is transmitted without noise, and the output symbol transmission times are equal. We introduce the timed Z-channel, where the output symbol transmission times are different.

Specifically, we show how the timed Z-channel applies to two examples of covert timing channel scenarios: a CPU scheduler, and a token ring network. We then give a detailed analysis of our timed Z-channel. We report a new result expressing the capacity of the timed Z-channel as the log of the root of a trinomial equation. This changes the capacity calculation from an optimization problem into a simpler algebraic problem and illustrates the relationship between the noise and time factors. Further, it generalizes Shannon's work on noiseless channels for this special case. We also report a new result bounding the timed Z-channel's capacity from below. Finally, we show how an interesting observation that Golomb reported for the Z-channel also holds for the timed Z-channel.

Title: Limitations on Design Principles for Public Key Protocols
Author(s): Paul F. Syverson
E-mail Address: syverson@itd.nrl.navy.mil
Citation: Proceedings of the 1996 IEEE Symposium on Security and Privacy, Oakland, CA, IEEE CS Press, pp62-73.
Date: May 1996
Report No.: CHACS-96-016

Abstract

Recent papers have taken a new look at cryptographic protocols from the perspective of proposing design principles. For years the main approach to cryptographic protocols has been logical, and a number of papers have examined the limitations of those logics. This paper takes a similar cautionary look at the design principal approach. Limitations and exceptions are offered on some of the previously given basic design principals. The focus is primarily on public key protocols, especially on the order of signature and encryption. But, other principles are discussed as well. Apparently secure protocols that fail to meet principles are presented. Also presented are new attacks on protocols as well as previously claimed attacks which are not.

Title: TAME: A Specialized Specification and Verification System for Timed Automate
Author(s): Myla M. Archer and Constance L. Heitmeyer
E-mail Address: heitmeyer@itd.nrl.navy.mil
Citation: Proceedings of Work in Progress session at RTSS '96, Wash, D.C., pp3-6
Date: December 4-6, 1996
Report No.: CHACS-96-017

Abstract

Assuring the correctness of specifications of real-time systems can involve significant human effort. The use of a mechanical theorem prover to encode such specifications and to verify their properties could significantly reduce this effort. A barrier to routinely encoding and mechanically verifying specifications has been the need first to master the specification language and logic of a general theorem proving system. Our approach to overcoming this barrier is to provide mechanical support for producing specifications and verifying proofs, specialized for particular mathematical models and proof techniques. We are currently

developing a mechanical verification system called TAME (Timed Automata Modeling Environment) that provides this specialized support using SRI's Prototype Verification System (PVS). Our system is intended to permit steps in reasoning similar to those in hand proofs that use model-specific techniques. TAME has recently been used to detect errors in a realistic example.

Title: Agent Safety and Security
Author(s): David M. Goldschlag, Carl E. Landwehr, and Michael G. Reed
E-mail Address: godschlag@itd.nrl.navy.mil or landwehr@itd.nrl.navy.mil or reed@itd.nrl.navy.mil
Citation: Macmillan Computer Publishing, (Chapter 23) in Bots and Other Internet Beasties, pp447-465
Date: Spring 1996
Report No.: CHACS-96-018

Abstract

Automobiles have proven to be a wonderful invention; people all over the world depend on them. However, cars used improperly can cause injuries - especially those that serve as hiding places for bombs. It is hard to imagine a software agent that could cause physical harm to anyone - it is only software, after all. What if that software controls an electrical appliance, such as a coffee maker? Could a control failure cause the coffee maker to overheat and start a fire?

Title: A Case Study of Two NRL Pump Prototypes
Author(s): Myong H. Kang, Ira S. Moskowitz, Bruce Montrose and James Parsonese
E-mail Address: mkang@itd.nrl.navy.mil or moskowitz@itd.nrl.navy.mil or montrose@itd.nrl.navy.mil or parsonese@itd.nrl.navy.mil
Citation: 12th Annual Computer Security Applications Conference, San Diego, CA. pp32-43
Date: Dec 1996
Report No.: CHACS-96-019

Abstract

As computer systems become more open and interconnected, the need for reliable and secure communication also increases. The NRL Pump was introduced to balance the requirements of reliability, congestion control, fairness, and good performance against those of threats from covert channels and denial of service attacks. In this paper, we describe two prototype efforts. One implements the Pump at the process (top) layer in terms of a 4-layer network reference model and the other implements the Pump at the transport layer. We then discuss lessons learned and how these lessons will be used in deciding upon the final hardware implementation of the Pump.

Title: A Framework for MLS Interoperability
Author(s): Myong H. Kang, Judith N. Froscher and Ira S. Moskowitz
E-mail Address: mkang@itd.nrl.navy.mil or froscher@itd.nrl.navy.mil or moskowitz@itd.nrl.navy.mil
Citation: IEEE High Assurance Systems Engineering Workshop, Niagara-on-the Lake
Date: Printed in a pre-proceedings in 1996. Final Proceedings to be published in Spring 1997
Report No.: CHACS-96-020

Abstract

Distributed object-oriented computing (DOC) is a new computing paradigm that promotes component-based development, location independence, scalability, software reuse, etc. Users of multilevel security (MLS) technology want to take advantage of these new technologies. However, the process of incorporating new technologies into MLS products is slower than the analogous process for non-secure commercial products because MLS products must go through rigorous evaluation/certification procedures. We propose an architectural framework that speeds up the process of introducing new technologies to MLS users. We examine the drawbacks of traditional MLS approaches and take a fresh look at the requirements of MLS users. We then introduce security-critical components that can enable MLS solutions and an MLS architectural framework that can accommodate not only legacy systems but also new technologies, including DOC, without jeopardizing system security. Our framework separates security critical components/functions from the rest of the system because these components must go through rigorous evaluation/certification processes. This approach enables the secure use of new technologies for MLS users.

Title: Proxies for Anonymous Routing
Author(s): Michael G. Reed, Paul F. Syverson, and David M. Goldschlag
E-mail Address: reed@itd.nrl.navy.mil or syverson@itd.nrl.navy.mil or goldschlag@itd.nrl.navy.mil
Citation: Proceedings of the 12th Annual Computer Security Applications Conference, San Diego, CA, pp95-104
Date: December 1996
Report No.: CHACS-96-021

Abstract

Using traffic analysis, it is possible to infer who is talking to whom over a public network. This paper describes a flexible communications infrastructure, *Onion Routing*, which is resistant to traffic analysis. *Onion Routing* lives just beneath the application layer, and is designed to interface with a wide variety of unmodified Internet services by means of proxies. *Onion Routing* has been implemented on Sun Solaris 2.4; proxies for WWW (HTTP) and TELNET have been implemented as well. Proxies for e-mail (SMTP) and FTP are forthcoming.

Onion Routing works in the following way: An application, instead of making a (socket) connection directly to a destination machine, makes a connection to an *Onion Routing Proxy* on some remote machine. That Onion Routing Proxy

builds a route through several other *Onion Routers* to the destination. Each Onion Router can only identify adjacent Onion Routers along the route. When the connection is broken, all information about the connection is cleared at each Onion Router. Data passed along the anonymous connection appears different at each Onion Router, so data caanot be tracked en route and compromised Onion Routers cannot cooperate.

Onion Routing differs from other anonymity services in two ways: Communication is real-time and bi-directional; and the anonymous connections are application independent. Onion Routing does not provide anonymity at the application layer. Applications may (and usually should) identify their users over the anonymous connection. However, the use of a packet switched public network should not automatically reveal who is talking to whom. This is the traffic analysis that Onion Routing complicates.

Title: Position Statement for New Paradigms for Internetwork Security Panel
Author(s): Steven Greenwald
Citation: Proceedings of 19th National Information Systems Security Conference, pp.698-700
Date: October 1996
Report No.: CHACS-96-023

Abstract

The security policy currently used on most distributed systems is an old one, dating back to simpler times when most computer systems were centralized. This security policy is based on the idea that there is a central managing authority, called the system administration, that is ultimately responsible for the management of compute security within an administrative domain. n this security policy system administration includes the management of system resources, user accounts, and user privileges. This security policy is typified by an operating system such as UNIX. I refer to this older security policy as the Jurassic Age Security Policy (JASP) since it apparently dates back to the time when huge dinosaur computers were kept in air-conditioned pens, lazily grazing on their data, before faster, leaner machines wiped them out.

Title: Architectural Considerations for Mobile Mesh Networking
Author(s): Scott M. Corson, Joseph P. Macker, and Steven G. Batsell
E-mail Address: macker@itd.nrl.navy.mil
Citation: Proceedings of IEEE Military Communications Conference, Vol. 1, pp225-229
Date: October 1996
Report No.: CHACS-96-024

Abstract

This paper describes the problem of routing and resource reservation in mobile mesh networks and presents architectural recommendations necessary for Internet Protocols to operate effectively in these environments. A "Mobile Mesh" network is an autonomous system of mobile routers connected by wireless links, the union of which forms an arbitrary graph. The routers are free

to move randomly; thus, the network's wireless topology may change rapidly and unpredictably.

Title: IVOX - The Interactive VOice eXchange Application
Author(s): Brian R. Adamson and Joseph P. Macker
E-mail Address: macker@itd.nrl.navy.mil
Citation: Naval Research Laboratory Formal Report NRL/FR/5520--96-9805
Date: February 1996
Report No.: CHACS-96-025

Abstract

A flexible, low data rate network voice terminal application and a set of new network integration techniques have been designed and developed at NRL for the support of real-time interactive voice communication over distributed, computer data networks. The NRL Interactive Vocie Exchange (IVOX) uses advanced voice compression techniques to maintain a low data rate throughput requirement. The low data rate feature of IVOX also allows for the use of voice communication over existing computer networks without a significant impact on the other data communications (e.g., e-mail, file transfer). IVOX provides a simple graphical user interface for call setup and management. IVOX allows for cross computer platform interoperability with versions for Sun SPARCStation, Silicon Graphics, and Hewlett Packard workstation. Since its conception and development, IVOX has become an operational fleet software component and has played a key role in numerous research projects and demonstrations. IVOX was adopted as a core feature of the Joint Deployed Intelligence Support System (JDISS). During 1995 Joint Warrior Interoperability Demonstration (JWID '95), IVOX successfully demonstrated integrated network voice capability between Tactical Aircraft Mission Planning System (TAMPS) and Common Operation Mission Planning and Support Strategy (COMPASS) workstation terminals. Additionally, IVOX was demonstrated from an operational NRL networking booth during the 1995 Armed Forces Communications and Electronics Association (AFCEA 95) convention. IVOX enhancements have been integrated into several research projects including the NRL Data and Voice Integration Advanced Technology Demonstration (DVI ATD) and the Common System NATO Interoperability (CSN) project.

Title: Controlled Link Sharing and Quality of Service Data Transfer for Military Internetworking
Author(s): Joseph P. Macker
E-mail Address: macker@itd.nrl.navy.mil
Citation: Proceedings of IEEE Military Communications Conference, Vol. 2, pp404-408
Date: October 1996
Report No.: CHACS-96-026

Abstract

This paper discusses system design issues related to enhancing present internet working architectures to achieve controlled link sharing and high assurance data interchange guarantees. The military services are implementing

both wired and wireless Internet Protocol (IP) based data networks to provide interoperable, heterogeneous network connectivity. At present, internetwork routing products forward network data traffic with limited concern for the link sharing policies or the specific quality requirements of the traffic flow. An enhanced Integrated Services IP architecture is emerging which provides solutions for a rich set of resource sharing requirements. We present an overview of this architecture and discuss performance issues for candidate system components in a military context. The strong conclusion is that, based upon recent research and emerging technologies, a dynamic mixture of guaranteed services and controlled link sharing is achievable over operational packet networks. We recommend future work to validate candidate servicing models and to understand military application, security, and policy management requirements within this enhanced architecture.

Title: Reliable Multicast Data Delivery for Military Networking
Author(s): Joseph P. Macker, J. Eric Klinker, and Scott M. Corson
E-mail Address: macker@itd.nrl.navy.mil
Citation: Proceedings of IEEE Military Communications Conference, Vol. 2, pp399-403
Date: October 1996
Report No.: CHACS-96-027

Abstract

Multicast networking support is becoming an increasingly important technology area for both commercial and military distributed or group-based networking applications. The underlying transport layer for IP multicast is presently the User Datagram Protocol (UDP) or raw IP datagrams. Both of these protocols provide a non-guaranteed, "best effort" delivery service. In the past, such delivery mechanisms have worked well for supporting traffic types insensitive to occasional lost or missing data (e.g., voice, video). An increasing variety of distributed multimedia applications are being developed in which reliable data delivery of all or a subset of data packets is a critical performance factor. As an example, distributed situational awareness applications play a major functional role in future military tactical internetworks. Reliable group file transfer (e.g., image dissemination) and interactive group planning systems are also emerging applications for integrated C4I networking. This paper describes the reliable multicast networking design problem and related protocol performance issues. A comprehensive coverage of presently available reliable multicasting protocols solutions is provided and performance tradeoffs are discussed. Two military application environments with diverse internetworking infrastructures and requirements are used as examples, Distributed Interactive Simulation (DIS) and wireless mobile networking. Recommendations are presented for reliable multicast processing related to both military application requirements and network architectures.

Title: Multicast Tree Construction in Directed Networks
Author(s): J. Eric Klinker
E-mail Address: klinker@itd.nrl.navy.mil
Citation: Proceedings of IEEE Military Communications Conference, Vol. 2, pp.496-500
Date: October 1996
Report No.: CHACS-96-028

Abstract

Significant interest exits within the military in moving towards an integrated services environment where traditional network services such as ftp, telnet, and e-mail can co-exits with real-time services such as voice, video, and satellite imagery. Multi cast routing is an effective means of providing the efficient utilization of network resources required to realize such an environment. Traditional multi cast routing algorithms assume a symmetric network topology. Many military communication assets are either asymmetric in their load or asymmetric in capacity (a good example is Direct Broadcast Satellite). In addition, many military communication assets are bandwidth constrained, and routing symmetrically may further contribute to congestion. Therefore, multi cast tree construction which tolerates network asymmetry is desirable for many military communication environments. This paper proposes an algorithm for constructing shared multi cast distribution trees in networks with asymmetric link capacities or loads. The algorithm tolerates asymmetry by building distinct, loop-free, sender and receiver paths onto a shared delivery tree. Additionally, the algorithm exhibits desirable security properties. Simulation results are presented that demonstrate the lower tree cost and better load balancing characteristics of the resultant trees over shortest path trees, with only a modest increase in path length.

Title: What is an Attack on a Cryptographic Protocol?
Author(s): Paul F. Syverson
E-mail Address: syverson@itd.nrl.navy.mil
Citation: Proceedings of the 9th IEEE Computer Security Foundations Workshop, p188
Date: June 1996
Report No.: CHACS-96-029

Abstract

Using traffic analysis, it is possible to infer who is talking to whom over a public network. This paper describes a flexible communications infrastructure, onion routing, which is resistant to traffic analysis. Onion routing lives just beneath the application layer, and is designed to interface with a wide variety of unmodified Internet services by means of proxies. Onion routing has been implemented on San Solaris 2.4; in addition, proxies for World Wide Web browsing (HTTP), remote logins (RLOGIN), e-mail (SMTP), and file transfers (FTP) have been implemented.

Onion routing provides application independent, real-time, and bi-directional anonymous connections that are resistant to both eavesdropping and traffic analysis. Applications making use of onion routing's anonymous connections may (and usually should) identify their users over the anonymous connection. User anonymity may be layered on top of the anonymous connections by removing identifying information from the data stream. Our goal here is anonymous connections, not anonymous communication. The use of a packet switched public network should not automatically reveal who is talking to whom. This is the traffic analysis that onion routing complicates.

Title: A New Security Policy for Distributed Resource Management and Access Control
Author(s): Steven J. Greenwald
Citation: Proceedings of IEEE New Security Paradigms Workshop
Date: September 1996
Report No.: CHACS-96-030

Abstract

The common security policies of access control and resource management are based upon a central managing authority, called the system administration, that is ultimately responsible for the management of a usage policy. This management is usually done with some combination of mandatory access control and discretionary access control methods, where each user is granted (or denied) privileges and resources depending on the usage policies enforced at that particular system. System administration includes the management of system resources, user accounts, and user privileges, This security policy is typified by an operating system such as UNIX, and it introduces several difficulties when working in a distributed computing environment.

This paper addresses distributed resource management and access control. It proposes a new version of the "Distributed Compartment Model" (DCM), first developed by Greenwald in his 1994 doctoral dissertation. DCM consists of two major components: *Handles*, a method for role based access control, and *Distributed Compartments*, a method allowing users to manage resources within a distributed system across administrative domain boundaries. This new version of DCM discussed in this paper is a refinement of the original formal security policy model. This paper concentrates on the history and background of the problems motivating the creation of DCM, describes the informal security policy, proposes some example scenarios as to how DCM could be used, and concludes with a discussion of the results of this research.

Title: Requirements and Approaches for a Computer Vulnerability Data Archive
Author(s): Bruce C. Gabrielson, Jeff D. Humphrey, and Carl E. Landwehr
E-mail Address: landwier@itd.nrl.navy.mil
Citation: Proceedings of the Workshop on Computer Vulnerability Data Sharing, NIST, Gaithersburg, MD
Date: 1996
Report No.: CHACS-96-031

Abstract

An archive for computer vulnerability information could benefit diverse communities, but those communities will impose different requirements on its use and form. We use "archive" rather than "repository" here to imply a place to store or retrieve information, regardless of its location, structure or form. This paper considers the requirements for such an archive from the perspective of three classes of stakeholders: providers, those who provide vulnerability information to an archive, subscribers, those who retrieve information from it, and the archive manager, who is responsible for maintaining its controls. The same individual or organization may be a member of two or even all three of these classes, but we need to distinguish the interests that arise from these different roles. After

considering the range of requirements that such an archive might satisfy, we review the current situation and suggest approaches to satisfy some of those requirements.

Title: OR/SM" A Prototype Integrated Modeling Environment Based on Structured Modeling
Author(s): Gordon P. Wright, Radha V. Mookerjee, Radha Chandrasckharan, N. Dan Worobetz, and Myong H. Kang
E-mail Address: mkang@itd.nrl.navy.mil
Citation: To appear in INFORMS, Journal of Computing
Date: September 1996
Report No.: CHACS-96-032

Abstract

This paper describes the design and implementation of OR/SM, a computerized modeling environment based on Structured Modeling. The uniqueness of OR/SM is in the following: (1) the use of ORACLE Tools and Database as the delivery platform; (2) an interactive link to QS (Quantitative Systems) - a commercial software package for solving a wide range of operations management models; and (3) automatic and interactive links to SAS, a powerful and widely used commercial statistical analysis software system and optimization solver. Some other key features are: (1) automatic generation of relational database tables for model data; (2) interactive checking of model syntax and semantics; and (3) automatic generation of several reference documents. An example each from inventory control and from marketing mix management are used to illustrate the capabilities of OR/SM.

Title: Consistency Checking of SCR-Style Requirements Specifications
Author(s): Constance L. Heitmeyer, Bruce Labaw, and Daniel Kiskis
E-mail Address: heitmeyer@itd.nrl.navy.mil or labaw@itd.nrl.navy.mil
Citation: Proceedings on the 2nd IEEE International Symposium on Requirements Engineering, York, England, pp56-63
Date: March 27-29, 1995
Report No.: CHACS-96-033

Abstract

This paper describes a class of formal analysis, called consistency checking, that mechanically checks requirements specifications, expressed in the SCR tabular notation for application-independent properties. Properties include domain coverage, type correctness, and determinism. As background, the SCR notation for specifying requirement's is reviewed. A formal requirements model describing the meaning of the SCR notation is summarized, and consistency checks derived from the formal model are described. The results of experiments to evaluate the utility of automated consistency checking are presented. Where consistency checking of requirements fits in the software development process is discussed.

Title: The Effects of Storage Jamming in Distributed Simulations
Author(s): John P. McDermott
E-mail Address: mcdermott@itd.nrl.navy.mil
Citation: Proceedings of the 14th Distributed Interactive Simulation Workshop, pp1115-1128
Date: March 1996
Report No.: CHACS-96-034

Abstract

Storage jamming attacks use Trojan horse software to reduce the quality of stored data, without being detected. Storage jamming can invalidate simulation results in ways that are hard to detect. Undetected invalid results can lead to the adoption of unrealistic doctrine or inappropriate procurements. Storage jamming is not prevented by network security mechanisms, conventional or MLS host access control, or cryptographic techniques. There are interim practices and specific mechanisms that can deter and detect storage jamming.

Title: A New Look at an Old Protocol
Author(s): Paul F. Syverson
E-mail Address: syverson@itd.nrl.navy.mil
Citation: ACM SIGOPS, Operating Systems Review Vol 30, No. 3., pp1-4
Date: July 1996
Report No.: CHACS-96-035

Abstract

Analyses of the Needham-Schroeder protocol using the logics SVO and BAN are discussed. It is shown that the protocol does not meet goals derived in the [BAN89] analysis of it . The features of SVO analysis revealing the inappropriateness of these goals are indicated.

Title: A Logical Approach to Multilevel Security of Probabilistic Systems
Author(s): James W. Gray III. and Paul F. Syverson
E-mail Address: syverson@itd.nrl.navy.mil
Citation: To appear in the Journal of Distributed Computing
Date: 1996
Report No.: CHACS-96-036

Abstract

We set out a modal logic for reason about multilevel security of probabilistic systems. This logic includes modalities for time, probability, and knowledge. Making use of the Halpern-Tutttle framework for reasoning about knowledge and probability, we give a semantics for our logic and prove it is sound. We give two syntactic definitions of perfect multilevel security and show that their semantic interpretations are equivalent to earlier, independently motivated characterizations. We also discuss the relation between these characterizations of security and between their usefulness in security analysis.

Title: A General Theory of Composition for a Class of 'Possibilistic' Properties
Author(s): John D. McLean
E-mail Address: mclean@itd.nrl.navy.mil
Citation: IEEE Transactions on Software Engineering, Vol 22, No. 1, pp53-67
Date: January 1996
Report No.: CHACS-96-037

Abstract

This paper presents a general theory of system composition for ``possibilistic'' security properties. We see that these properties fall outside of the Alpern-Schneider safety/liveness domain and, hence, are not subject to the Abadi-Lamport Composition Principle. We then introduce a set of trace constructors, called ``selective interleaving functions,'' and show that possibilistic security properties are closure properties with respect to different classes of selective interleaving functions. This provides a uniform framework for analyzing these properties and allows us to construct a partial ordering for them. We present a number of composition constructs, show the extent to which each preserves closure with respect to different classes of selective interleaving functions, and show that they are sufficient for forming the general hook-up construction. We see that although closure under a class of selective interleaving functions is generally preserved by product and cascading, it is not generally preserved by feedback, internal system composition constructs, or refinement. We examine the reason for this.

Title Formal Methods for Real Time Computing
Author(s): Constance L. Heitmeyer and Dino Mandrioli (eds)
E-mail Address: heitmeyer@itd.nrl.navy.mil
Citation: Book published by John Wiley & Sons Trends in Software Series, v5, New York, 1996
Date: 1996
Report No.: CHACS-96-038

Title: Formal Methods for Real-Time Computing: A Overview
Author(s): Constance L. Heitmeyer and Dino Mandrioli
E-mail Address: heitmeyer@itd.nrl.navy.mil
Citation: Book chapter in Formal Methods for Real-Time Computing, John Wiley, New York, 1996, pp1-32
Date: 1996
Report No.: CHACS-96-039

Abstract

This chapter defines real-time systems and illustrates them with a number of small examples. It also discusses issues central to applying formal methods in the development of real-time systems: the trade-offs between operational and descriptive specifications, different levels of formality that can be applied, and the requirements of formal methods for building industrial-strength systems. To put the newer formal methods into perspective, two methods widely used in practice to design and analyze real-time systems, namely, structured analysis and

Statecharts, are reviewed. Several promising new techniques for specifying and analyzing real-time systems are then summarized and illustrated with examples. These include graphical notations, state machine and logic-based models, process algebras, and analysis techniques, such as model checking and deductive reasoning.

Title: Formal Methods for Verifying Real-Time Systems Using Timed Automatation
Author(s): Constance L. Heitmeyer and Nancy Lynch
E-mail Address: heitmeyer@itd.nrl.navy.mil
Citation: Book chapter in Formal Methods for Real-Time Computing, John Wiley, New York, 1996, pp83-106
Date: 1996
Report No.: CHACS-96-040

Abstract

The use of the Lynch-Vaandrager timed automaton model is illustrated with a solution to the Generalized Railroad Crossing problem. The solution shows formally the correspondence between four system descriptions: an axiomatic (i.e., descriptive) specification, an operational specification represented in terms of timed automata, a discrete system implementation, and a system implementation that works with a continuous gate model. Several sample proofs are given. In the development of the solution, a number of guidelines were applied. These guidelines, which should prove useful in applying formal methods to practical systems, are described and illustrated with examples.

Title: Applications of Private Socket Connections
Author(s): Michael G. Reed, Paul F. Syverson, and David M. Goldschlag
E-mail Address: reed@itd.nrl.navy.mil or syverson@iitd.nrl.navy.mil or goldschlag@itd.nrl.navy.mil
Citation: Proceedings of the 4th Annual ACM Conference on Computer and Communications Security, Zurich, Switzerland, ACM press
Date: 1996
Report No.: CHACS-96-041

Abstract

Onion Routing [10, 16] provides a new primitive, *private socket connections*. These private connections are strongly resistant to both eavesdropping and traffic analysis. By removing identifying information from the data stream, these connections may be made anonymous. A prototype of onion routing is in the public domain. This paper describes applications of onion routing; onion routing proxies for RLOGIN, HTTP, SMTP, and FTP; private connections that hide location information for cellular phone and location tracking systems, and other Internet applications.

Title: A New Approach to Secure Distributed Computation
Author(s): Paul F. Syverson
E-mail Address: syverson@itd.nrl.navy.mil
Citation: Proceedings of the New Security Paradigms Workshop, Lake Arrowhead, CA, IEEE CS Press
Date: September 16-19, 1996
Report No.: CHACS-96-042

Abstract

A model of secure distributed computation is given in which friendly and hostile nodes are represented in competing interwoven networks of nodes. This is intended to provide a more realistic model of distributed computation than the usual worst-case models. It is suggested that reasoning about goals, risks, tradeoffs, etc. for this model be done in a game-theoretic framework.

Title: An Epistemic Model for Cryptographic Protocol Analysis
Author(s): Paul F. Syverson
E-mail Address: syverson@its.nrl.navy.mil
Citation: Proceedings of the Theoretical Aspects of Rationality and Knowledge (TARK VI), De Zeeuwse Stromen, The Netherlands
Date: March 17-20, 1996
Report No.: CHACS-96-043

Abstract

We present a model of computation and of knowledge for cryptographic protocols. These serve as a semantics for a logic in the BAN family, SVO, with respect to which that logic is sound. We compare our model of computation to another associated with the NRL Protocol Analyser. By showing how to associate the models we provide a basis for a unified analysis in which each analysis tool can do what it does best against the backdrop of a single model. We also briefly discuss the relation between the presented model and one due to Merritt.

Title: Descriptive Top-Level Specifications: A Chapter of the Handbook for the Computer Security Certification of Trusted Systems
Author(s): John P. McDermott
E-mail Address: mcdermott@itd.nrl.navy.mil
Citation: Code 5540 WWW Page
Date: 1996
Report No.: CHACS-96-044

Abstract

This report is one chapter of the NRL Handbook for Computer Security Certification of Trusted Systems. Other chapters of the Handbook are published in NRL Reports or Technical Memoranda. This report assumes that the reader is already familiar with the development of untrusted Navy systems as discussed in [13] and with the *DoD Trusted Computer System Evaluation Criteria* [12], also

known as the Orange Book. If the reader does not have prior experience in system development of any kind, then he or she needs to do some background study in that area to get maximum benefit from this report.

This chapter is written for evaluators. It discusses how one might evaluate a descriptive top-level specification (hereafter called a DTLS) for a trusted system. It does not directly address how one might develop a trusted system and it does not provide standards for DTLSs.

This chapter necessarily omits a critical part of the evaluation process, the trusted application itself. Each application has a significant impact on security. The definition of security and the kinds of mechanisms used will change from application to application. Because applications are application dependent we cannot discuss them here. Nevertheless, it is not possible to build or evaluate trusted sytems without understanding the application.

The chapter is organized into three sections. The first two sections are written for technical managers and executives. They define the DTLS in terms of its use, its quality, and its relationship to other system development concepts. They asume that the reader is a technical manager who knows about untrusted system development but is encountering a trusted system development project for the first time. The third section is written with the certification team in mind. It discusses how a certification team might go about evaluating a DTLS in terms of what they would be looking for and how they might find it. The third section assumes that the reader has some experience in system development, including some knowledge of system, software, and hardware engineering in these kinds of projects.

Title: Secure Broadcast Using Secure Coprocessors
Author(s): David M. Goldschlag
E-mail Address: goldschlag@itd.nrl.navy.mil
Citation: Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, IEEE Press
Date: May 6-8, 1996
Report No.: CHACS-96-045

Abstract

This paper describes an efficient and flexible solution to the problem of secure broadcast. Messages need be encrypted only once, independent of the size of the broadcast group, and recipients may be easily added to or dropped from the broadcast group, without the need to inform the rest of the group. The solution is novel because it integrates simple cryptographic protocols with secure coprocessors. Secure coprocessors are hardware devices that can be trusted both to carry out specified functions, and to keep secrets, even in the face of malicious tempering. Although these assumptions are quite strong, they are reliable. The ability to trust a part of a system adds considerable flexibility into the design space, and can result in a more practical system.

Title: Secure Information Through Replicated Architecture (SINTRA)
Author(s): Judith N. Froscher
E-mail Address: froscher@itd.nrl.navy.mil
Citation: Handbook of Data Management, AUERBACH
Date: 1996
Report No.: CHACS-96-946

Abstract

As information systems that process and manage national security, financial, medical, and other sensitive data become more highly interconnected and more accessible to a community of users with diverse backgrounds. Those sytems must also ensure that users have access to all and only the information for which they are authorized. Such systems are multilevel secure (MLS). Developing software that can be trusted to enforce such security requirements, however, has proven quite difficult in practice and results in security technology that is often outdated. The SINTRA approach to database security relies on physical separation to provide strong protection and replication to allow users with different security authorizations access to data created at a less restricted security level. Because this approach exploits distribution and replication to provide a secure data management service, it allows critical information systems both to exploit commercial advances in data management technology and to protect sensitive information at the same time. Each node in a SINTRA confederation is a commercially available data management system, but the confederation itself is secure. A simple, strong, reliable store-and-forward device provides the protection critical component and is reusable with other transactional systems. The SINTRA approach provides an affordable, strong approach to the protection of critical information and allows both government and commercial enterprises to take advantage of the commercial investment in information technology.

1995 PUBLICATIONS

CHACS-95-001 Epistemology of Information Flow in the Multilevel Security of Probabilistic Systems, *James W. Gray, III*

CHACS-95-002 Software Requirements: A Tutorial, *Stuart R. Faulk*

CHACS-95-003 Security for the Internet Protocol, *Randall J. Atkinson*

CHACS-95-004 External COMSEC Adaptor Software Engineering Methodology, *Andrew Moore, Eather Chapman, et al.*

CHACS-95-005 A Data Pump for Communication, *Myong H. Kang and Ira S. Moskowitz*

CHACS-95-006 Improving Inter-Enclave Information Flow for a Secure Strike Planning Application, *Judith N. Froscher, et. Al.*

CHACS-95-007 SCR*: A Toolset or Specifying and Analyzing Requirements, *C. Heitmeyer, A. Bull, C. Gasarch, and B. Labaw*

CHACS-95-008 A Network Pump, Myong Kang, *Ira S. Moskowitz and Daniel C. Lee*

CHACS-95-009 Storage Jamming, *John McDermott and David Goldschlag*

CHACS-95-010 One Time Passwords In Everything (OPIE): Experiences with Building and Using Strong Authentication, *Daniel L. McDonald, R. J. Atkinson, and C. Metz*

CHACS-95-011 High Assurance Computer Systems: A Research Agenda, America in the Age of Information, *John D. McLean and C.L. Heitmeyer*

CHACS-95-012 Applying the Dependability Paradigm to Computer Security, *Catherine A. Meadows*

CHACS-95-013 Using Temporal Logic to Specify and Verify Cryptographic Protocols (Progress Report), *James W. Gray, III and J.D. McLean*

CHACS-95-014 The NRL Protocol Analyzer: An Overview, *Catherine A. Meadows*

CHACS-95-015 Formal Verification of Cryptographic Protocols: A Survey, *Catherine Meadows*

CHACS-95-016 Integrity in Multilevel Secure Database Management Systems, *Catherine A. Meadows and Sushil Jajodia*

CHACS-95-017 Inference Problems in Multilevel Secure Database Management Systems, *Sushil Jajodia and Catherine Meadows*

CHACS-95-018 The Role of Trust in Information Integrity Protocols, *Gustavus Simmons and Catherine Meadows*

CHACS-95-019 The Modulated-Input Modulated-Output Model, *Ira S. Moskowitz and Myong Kang*

CHACS-95-020 Reduction of a Class of Fox-Wright Psi Functions for Certain Rational Parameters, *Allen R. Miller and Ira S. Moskowitz*

CHACS-95-021 A Network Version of the Pump, *Myong H. Kang, Ira S. Moskowitz and Daniel C. Lee*

CHACS-95-022 Assurance Mappings, A Chapter of the Handbook for the Computer Security Certification of Trusted Systems, *J. McHugh, C.N. Payne, and C. Martin*

CHACS-95-023 Security Policy Model , A Chapter of the Handbook, for the Computer Security Certification of Trusted Systems, *Charles N. Payne*

CHACS-95-024 The Epistemic Representation of Information Flow Security in Probabilistic Systems, *Paul F. Syverson and James W. Gray, III*

CHACS-95-025 Fail Stop Protocols: An Approach to Designing Secure Protocols, *Li Gong and Paul F. Syverson*

1994 PUBLICATIONS

CHACS-94-001 Confidentiality in a Replicated Architecture Trusted Database System: A Formal Model, *O. Costich, J. D. McLean, and J. P. McDermott*

CHACS-94-002 The SINTRA Data Model: Structure and Operations, *O. Costich, M. H. Kang, and J. N. Froscher*

CHACS-94-003 A Practical Approach to High Assurance Multilevel Secure Computing Service, *J. N. Froscher, M. H. Kang, J. P. McDermott, O. Costich, and C. E. Landwehr*

CHACS-94-004 Multiple-query Optimization at Algorithm-level, *M. H. Kang, H. Dietz, and B. Bhargava*

CHACS-94-005 Architectural Impact on Performance of a Multilevel Database System, *M. H. Kang and J. N. Froscher*

CHACS-94-006 Achieving Database Security through Data Replication: The SINTRA Prototype, *M. H. Kang, J. N. Froscher, J. P. McDermott, O. Costich, and R. Peyton*

CHACS-94-007 Using Object Modeling Techniques To Design MLS Data Models, in Security for Object-Oriented Systems, *M. H. Kang, O. Costich, and J. N. Froscher*

CHACS-94-008 A Taxonomy of Computer Program Security Flaws, with Examples, *C. E. Landwehr, A. R. Bull, J. P. McDermott, and W. S. Choi*

CHACS-94-009 Hidden Safety Requirements in Large-scale Systems, *C. E. Landwehr*

CHACS-94-010 The B2/C3 problem: How Big Buffers Overcome Covert Channel Cynicism in Trusted Database Systems, *J. P. McDermott*

CHACS-94-011 Covert Channels—Here to Stay?, *I. S. Moskowitz and M. H. Kang*

CHACS-94-012 Discussion of a Statistical Channel, *I. S. Moskowitz and M.H. Kang*

CHACS-94-013 An Experience Modeling Critical Requirements, *C. N. Payne, A. P. Moore, and D. M. Mihelcic*

CCHAS-94-014 An Epistemic Logic of Situations, *P. Syverson,*

CHACS-94-015 On Unifying Some Cryptographic Protocol Logics, *P. Syverson and P. van Oorschot*

CHACS-94-016 A Taxonomy of Replay Attacks, *P. Syverson*

CHACS-94-017 The NRL Protocol Analyzer: An Overview, *C.A. Meadows*

CHACS-94-018 A Model of Computation for the NRL Protocol Analyzer, *C.A. Meadows*

CCHAS-94-019 Three Systems for Cryptographic Protocol Analysis, *R. Kemmerer, C.A. Meadows, and J. Millen*

CHACS-94-020 Tradeoff Areas in Secure System Development, *C.A. Meadows*

CHACS-94-021 Formal Requirements for Key Distribution Protocols, *P. Syverson and C.A. Meadows*

CHACS-94-022 The Feasibility of Quantitative Assessment of Security, *C.A. Meadows*

CHACS-94-023 The Need for a Failure Model for Security, *C.A. Meadows*

CHACS-94-024 Mechanically Verifying Safety and Liveness Properties of a Delay Insensitive FIFO Queue, *D.M. Goldschlag*

CHACS-94-025 A Formal Model of Several Fundamental VHDL Concepts, *D.M. Goldschlag*

CHACS-94-026 Simple Timing Channels, *I.S. Moskowitz and A. Miller*

CHACS-94-027 Detailed Operational Concept for the JTIDS Key Management System, *S. S. Shah*

CHACS-94-028 Modechart Toolset User's Guide, *A.T. Rose, M.A. Pérez, and P.C. Clements*

CHACS-94-029 A Toolset for Developing Real-Time Systems, *C. Heitmeyer*

CHACS-94-030 A General Theory of Composition for Trace Sets Closed Under Selective Interleaving Functions, *J.D. McLean*

CHACS-94-031 Assurance Risk Assessment and Fuzzy Logic, *J.D. McLean*

CHACS-94-032 Security Models, *J.D. McLean*

CHACS-94-033 Quantitative Measures of Security, *J.D. McLean*

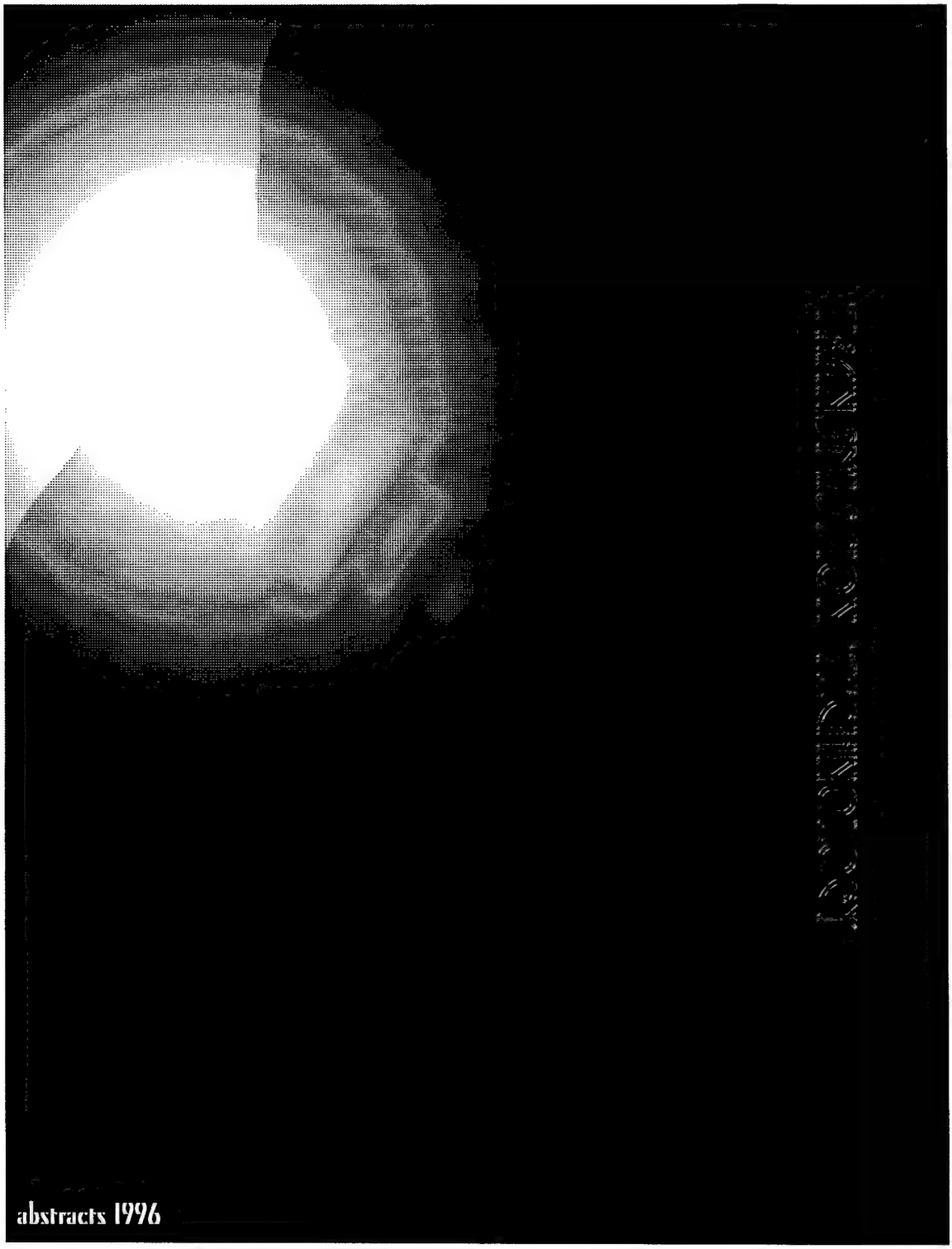
CHACS-94-034 The Generalized Railroad Crossing: A Case Study in Formal Verification of Real-Time Systems, *C.L. Heitmeyer and N. Lynch*

CHACS-94-035 The Generalized Railroad Crossing: A Case Study in Formal Verification of Real-Time Systems, *C.L. Heitmeyer and N. Lynch*

CHACS-94-036 The Role of HCI in CASE Tools Supporting Formal Methods, *C.L. Heitmeyer*

CHACS-94-037 CAROL (CES2300 Phase II Rooftop Test Results (U)), *P.M. Jenket*

CHACS-94-038 Design Documentation for the SINTRA Preprocessor, *Myong H. Kang and Rodney Peyton*


abstracts 1996

TRANSMISSION TECHNOLOGY

CODE 5550

The Transmission Technology (TT) Branch conducts a research and development program directed toward the improvement of information transmission and reception between surface, air, submerged and space platforms. The Branch mission includes understanding and developing approaches to satisfy the need for affordable, efficient and robust dissemination of combat management information. In support of this goal, the Branch investigates all aspects of the process of information transfer including the development of state-of-the-art transmission equipment as well as research into antennas and channel propagation phenomena. Emphasis is placed on those aspects of transmission technology that permit adaptation to inhospitable natural or man-made environments. In addition, the Branch conducts research and development in support of signal intercept and related intelligence system projects. Areas of activity include: (1) wideband HF architecture and RF system engineering; (2) communication channel characterization including Arctic communication issues; (3) intercept system analysis, development, and prototype evaluation; (4) satellite and space communication technology; and (5) research into wideband and compact antenna systems.

Title: Data Telemetry and Acquisition System for Acoustic Signal Processing Investigations
Author(s): Michael A. Rupar, Joseph A. Goldstein and Timothy L. Krout
E-mail Address: rupar@itd.nrl.navy.mil or goldstein@itd.nrl.navy.mil or krout@abyss.nrl.navy.mil
Citation: Naval Research Laboratory Memorandum Report, NRL/MR/5550--96-7820
Date: February 20, 1996
Report No: TT-96-001

Abstract

This report describes the Satellite Vertical Line Array 32-channel system (SVLA-32) developed at the Naval Research Laboratory (NRL) for use during open ocean acoustic signal processing investigations for remote data collection and system control. This system was used during the TTCP Environmental Signal Processing Experiment (TESPEX) exercises in the summer of 1994, and demonstrated its ability to provide real-time collection of acoustic data over 32 channels, to perform onsite data formatting and the satellite transfer of that data to shore, and to allow full system command and control via the same satellite link. The system can be divided into the following subsystems: (1) the in-water subsystem: a hydrophone array, data acquisition unit, and umbilical cable, (2) the signal processing and recording subsystem, responsible for data formatting, storage to recording devices, and data dissemination, (3) the satellite communication subsystem, responsible for data telemetry and for remote control of the ocean buoy from the shore data processing center, and (4) the buoy subsystem, which includes a primary power generator and a buoy weather station. Capabilities of the current system are described as well as lessons learned during the TESPEX II program.

Title: Performance Issues of ISDN Voice Communication within the U.S. Navy
Author(s): David Heide and Lawrence Fransen
E-mail Address: heide@itd.nrl.navy.mil or fransen@itd.nrlnavy.mil
Citation: ICSAAT, Conference Proceedings, Vol. 2, p21
Date: October 9, 1996
Report No: TT-96-002

Abstract

There is considerable interest in the U.S. Navy to update analog voice circuits with Integrated Services Digital Network (ISDN) technology, particularly shipboard environment. A goal of the Voice Systems Section of the Naval Research Laboratory (NRL) is to develop voice algorithms that achieve superior intelligibility, acceptability, and speaker recognizability in noisy environments with constrained data rates. This experience is now being used to investigate the best approach for incorporating speech technology into ISDN for use in Navy platforms.

One of the possible approaches for improving speech quality is to extend the speech bandwidth above the conventional 4 kHz. Thus, the focus of this report will be on comparing higher bandwidth algorithms for use in high noise environments like those found in the Navy. We conducted formalized quality and

intelligibility tests of voice algorithms compatible with ISDN under various Navy noise environments. Our study addresses the inherent loss of intelligibility that occurs when speech is typically low-pass filtered below 4 kHz prior to sampling at 8 kHz.

Our testing indicates that speech quality and intelligibility in a quiet environment is improved for a significant percentage of the population by using an 8 kHz bandwidth. In noisy environments, higher bandwidth speech results in even greater intelligibility improvement. In particular, the female voice benefits the most when a higher bandwidth is used. Best results are not achieved by the standard 4 kHz bandwidth pulse code modulation (PCM) operating at 64 kilobits per second (kbps). An 8 kH z bandwidth system such as the 64 kbps sub-band adaptive differential pulse code modulation (SB-ADPCM) achieves superior overall speech quality and intelligibility.

Ttile: Narrowband Multimedia Briefing Device
Author(s): Thomas M. Moran and George S. Kang
E-mail Address: moran@itd.nrl.navy mil or kang@itd.nrl.navy mil
Citation: ICSAAT Conference Proceedings, Vol. 2, pp1292-1296
Date: October 9, 1996
Report No: TT-96-003

Abstract

Naval tactical communicators rely primarily on narrowband voice channels. Even though certain tactical users have the capability for image transmission, there is no single device providing multimedia communication for narrowband, tactical users. Multimedia communication usually implies video conferencing and a requirement for a large amount of transmission bandwidth. While this is obviously not practical at the low data rates available to tactical communicators, a multimedia communications device, properly designed to minimize data transmission, would be a valuable asset to tactical communicators. In this paper, we describe such a device which we call the Narrowband Multimedia Briefing Device.

1995 PUBLICATIONS

TT-95-001 Delay, Doppler, and Amplitude Characteristics of HF Signals Received Over a 1300-km Transauroral Skywave Channel, *Leonard S. Wagner, Joseph A. Goldstein, Michael A. Rupar and Edward J. Kennedy*

TT-95-002 Channel Spread Parameters for the High-Latitude, Near-Vertical-Incidence-Skywave HF Channel: Correlation with Geomagnetic Activity, *Leonard S. WagneR, and Joseph A. Goldstein*

TT-95-003 2.4-kb/s Vocoder Based on Pitch-Synchronous Segmentation of Speech, *George S. Kang and Lawrence J. Fransen*

TT-95-004 Protocol Profiles for Near-Term ATM Usage, *Lynn M. Koffley and Donald G. Kallgren*

1994 PUBLICATIONS

TT-94-001 Enhancement of Stimulated Electromagnetic Emission during Two Frequency Ionospheric Heating Experiments, *Paul A. Bernhardt, Leonard S. Wagner, Joseph A. Goldstein, et al.*

TT-94-002 Correlation of High Latitude Lonospheric Disturbances with Geomagnetic Activity, *Leonard S. Wagner and Joseph A. Goldstein*

TT-94-003 Encoded Speech Intelligibility Improvement in the F/A-18 Noise Environment Using Spectral Subtraction Preprocessing, *David A. Heide*

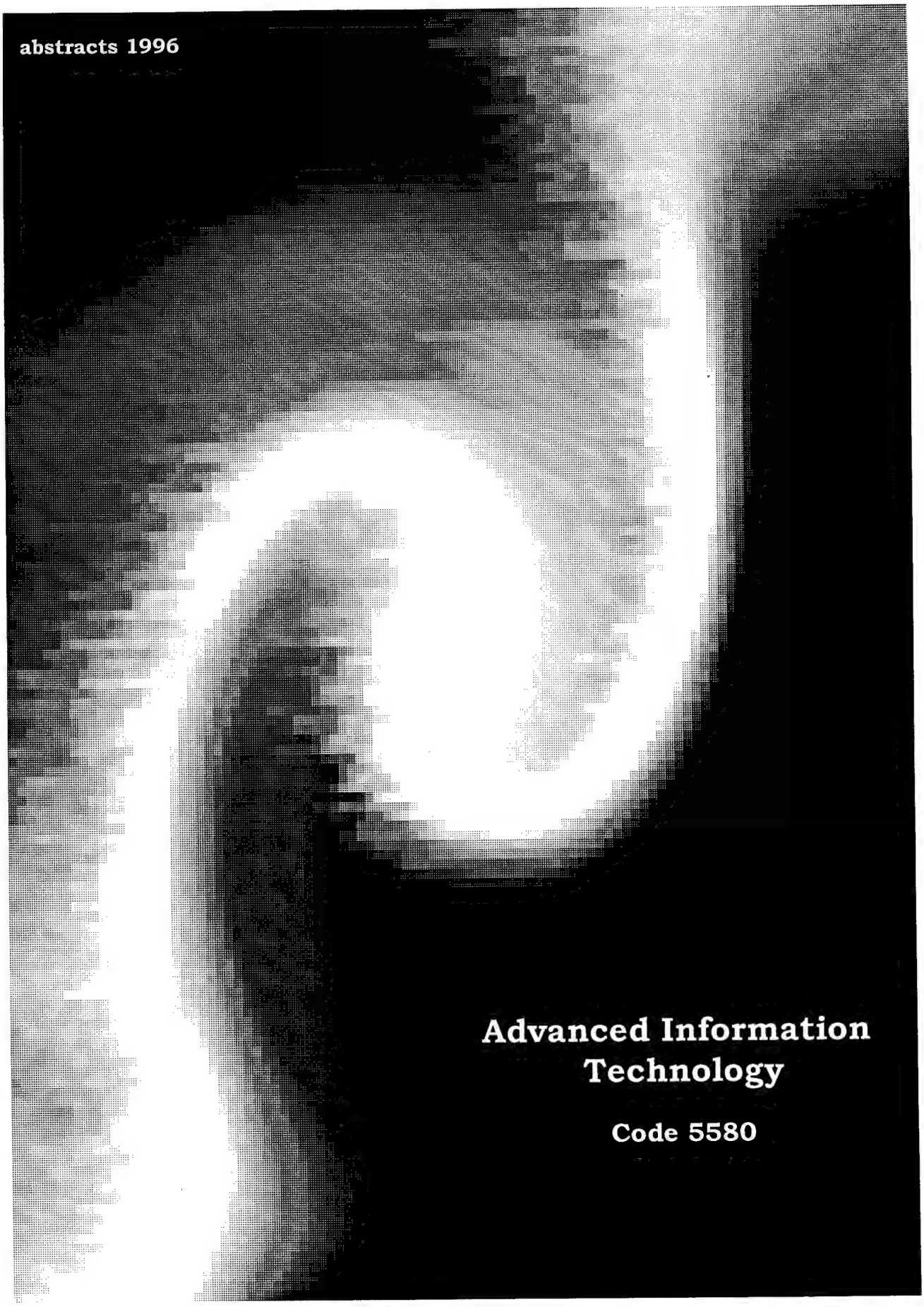
TT-94-004 Arctic Propagation Phenomena at VHF and UHF for a BLOS Path, *Edward J. Kennedy and Michael A. Rupar*

TT-94-005 Speech Analysis and Synthesis Based on Pitch-Synchronous Segmentation of the Speech Waveform, *George S. Kang and Lawrence J. Fransen*

TT-94-006 Electromagnetic Spectrum Occupancy Study of a Potential Transmitter Site for the HF Active Auroral Research Program (HAARP), *Joseph A. Goldstein, Edward J. Kennedy and Monroe Y. McGown*

TT-94-007 A Laboratory Prototype HF Repeater for Relocatable Over-the-Horizon-Radar, *Adrian S. Eley*

TT-94-008 TESPEX 2: Data Telemetry and Acquisition, *Timothy L. Krout , Jon Jannucci, Joseph Goldstein, et al.*


abstracts 1996
Advanced Information Technology
Code 5580

ADVANCED INFORMATION TECHNOLOGY

CODE 5580

The Advanced Information Technology (AIT) Branch of the Information Technology Division develops and implements cutting edge hardware and software solutions to Navy problems in a number of application areas. Current research and development thrusts include:

- parallel and distributed hardware, software and display technologies;
- novel signal processing techniques directed primarily toward the exploitation of massively parallel systems;
- development of hardware-independent systems for developing and porting code for parallel processing systems;
- design and implementation of reactive and interactive control systems;
- development of technologies for decision support systems and prototyping of all varieties of decision systems including tactical decision aids and mission planning;
- exploration and demonstration of new methods for data management including data fusion, design and navigation of database systems, and correlation and tracking of current and historical information; and display technologies for visual management of all of the above applications.

The technical programs in the Branch include some basic research (6.1), a substantial exploratory development program (6.2) and a continuing effort to field technology through a succession of advanced technology demonstrations (6.3a). The Branch draws on expertise in computer science, mathematics, operations research, electrical engineering and physics.

Title: Beasties and Other Bots
Author(s): James B. Hofmann
E-Mail Address: hofmann@ait.nrl.navy.mil
Citation: Published in Internet-based Software Agents Book, Chapter XVII, pp318-338
Date: May 1996
ITD Report No.: AIT-96-002

Abstract

What impact does software agent technology have on military doctrine and future concepts of operation? Will the proliferation of agents on secure military computer networks help or hinder the warfighter in his mission? Will software agents contribute to problems associated with "information overload," or will they reduce the vast amounts of raw data by converting them into useful, tailored information? Can agents provide and operate in non-benign military environments characterized by limited bandwidth, noisy and frequently interrupted communications, and an infrastructure that is vulnerable to information-based attacks? This chapter examines the current revolution in military affairs and illustrates how software agent technology will have its greatest impact solving both the age-old problems that have long besieged the military and the newer problems caused by increasing reliance on information in modern warfare.

Title: Synthetic Database Methods
Author(s): Karen A. Erner
E-Mail Address: erner@ait.nrl.navy.mil
Citation: Naval Research Laboratory Formal Report, NRL/FR/5580--96-9810
Date: Mar. 27, 1996
Report No.: AIT-96-003

Abstract

In this report, I develop methods for the generation of a synthetic database, whose records may include fields of different types including text strings, characters, and numbers. I examine techniques allowing us to simulate particular frequency distributions for each field in a data record and to reflect relations between the fields in a data record. In addition, to produce more realistic looking text data, I also present an elementary algorithm that generates key entry or typographical errors.

Title: VHDL-Based Performance Modeling for the Processing Graph Method Tool (PGMT) Environment
Author(s): Roger Hillson, David J. Kaplan, Robert Klenke, and James Aylor
E-Mail Address: hillson@ait.nrl.navy.mil or kaplan@ait.nrl.navy.mil
Citation: Published in the Proceedings of the VHDL International Users Forum (VIUF), pp69-78
Date: February 28 - March 2, 1996
Report No.: AIT-96-005

Abstract

Applications that execute on high performance multiprocessors often must meet stringent real-time constraints. The interaction of the applications, the runtime scheduler, and the multiprocessor architecture will have a significant impact on performance. This paper presents an outline of the efforts of the Center for Semicustom Integrated Systems and the Naval Research Laboratory to develop a performance modeling environment for processing graphs running on multiprocessors. VHDL is used to model the target multiprocessor architecture. A scheduler written in C or C++ is used to assign transitions, which are the computational elements in the processing graph, to subprocessors in the VHDL hardware model. This assignment process may be dynamic. The transition's execution time can be estimated as a function of its input parameters through the application of multivariate regression techniques. The transition's estimated execution time is passed from the scheduler to the VHDL hardware model when the transition is assigned to a subprocessor. The transition's timing may vary on a successive executions if the transition's input parameters change. The interaction between the scheduler and the VHDL model takes place through a VHDL-to-C interface.

Title: Fuzzy-Algebra Uncertainty Assessment
Author(s): J. Arlin Cooper and Douglas K. Cooper
E-Mail Address: cooper@ait.nrl.navy.mil
Citation: Proceedings of the 7th Workshop of Neural Networks, Fuzzy Systems and Virtual Reality
Date: 1996
Report No.: AIT-96-006

Abstract

A significant number of analytical problems (for example, abnormal-environment safety analysis) depend on data that are partly or mostly subjective. Since fuzzy algebra depends on subjective operands, we have been investigating its applicability to these forms of assessment, particularly for portraying uncertainty in the results of PRA (probabilistic risk analysis) and in risk-analysis-aided decision-making. Since analysis results can be a major contributor to a safety-measure decision process, risk management depends on relating uncertainty to only know (not assumed) information. The uncertainties, due to abnormal environments, are even more challenging than those in normal-environment safety assessments; and therefore require an even more judicious approach. Fuzzy algebra matches these requirements well.

One of the most useful aspects of this work is that we have shown the potential for significant differences (especially in perceived margin relative to a decision threshold) between fuzzy assessment and probabilistic assessment based on subtle factors inherited in the choice or probability distribution models. We have also shown the relation of fuzzy-algebra assessment to "bounds" analysis, as well as a description of how analyses can migrate from bounds analysis to fuzzy-algebra analysis, and to probabilistic analysis as information about the process to be analyzed is obtained. Instructive examples are used to illustrate the points.

Title: Estimating the Effective Depth of Laser Imaging Systems in Various Ocean Environments.
Author(s): Jerry L. Gorline
E-Mail Address: gorline@ait.nrl.navy.mil
Citation: Naval Research Laboratory Formal Report, NRL/FR/5580--96-9809
Date: May 9, 1996
Report No.: AIT-96-009

Abstract

In this paper we present the results of running Monte Carlo simulations on the Connection Machine (CM-5E) to study the behavior of laser propagation in the ocean. We developed an advanced hydrolic radiative transfer model to estimate the effective depth of a laser imaging systems in various ocean environments. This model simulates a flat ocean surface. The effective depth is defined as that at which a six-pixel wide disk target can no longer be detected in the upward irradiance field at the ocean surface. Simulations showed that the effective depth was inversely proportional to the total attenuation coefficient.

Title: Dynamic Route Optimization with Time-Expanded Graphs
Author(s): Miguel R. Zuniga
E-Mail Address: zuniga@ait.nrl.navy.mil
Citation: Proceedings of the 10th Annual International SPIE Aerospace Symposium
Date: April 8-12, 1996
Report No.: AIT-96-010

Abstract

An important computer calculation in military planning is determining the optimal paths that a set of flying objects (airplanes, cruise missiles, UAVs) should take toward their targets. The current practice is to represent the problem with static graphs, then apply search algorithms (e.g. network flow) that can yield least cost paths. A number of significant problems must be solved in order to determine optimal and realistic paths. These include the difficulty associated with representing dynamic (time dependent) and realistic phenomenon, and the associated difficulties of solving the graphs with polynomial-time algorithms.

In this paper we discuss the limitations of modeling with graph theoretic techniques, and we present some results that permit significantly more accurate problem representation and solution than the previous state of the art. These include: a new method for graph representation of dynamic of phenomenon associated with strike routing; some general relations that are important in modeling with graphs whose edge traversals represent independent probabilistic events; and a number of new models for use in optimizations. Some of the issues and solutions that we present are very general, and they are also given detailed discussion in the context of two important military problems: general radar detection representation for optimization, and representation of the overflight problem (the increased threat to strike assets as they repeat flights over threats). Finally, the models and algorithms are considered in relation to single asset routing and joint routing of multiple assets.

Title: General Data Fusion for Estimates with Unknown Cross Covariances
Author(s): Jeffrey K. Uhlmann
E-Mail Address: uhlmann@ait.nrl.navy.mil
Citation: Proceedings of the 10th Annual International SPIE Aerospace Conference
Date: April 8-12. 1996
Report No.: AIT-96-011

Abstract

In this paper we present a new theoretic framework for combining sensor measurements, state estimates, or any similar type of quantity gives only their means and covariances. The key feature of the new framework is that it permits the optimal fusion of estimates that are correlated to an unknown degree. This framework yields a new filtering paradigm that avoids all of the restrictive independence assumptions required by the standard Kalman filter, though at the cost of reduced rates of convergence for cases in which independence can be established.

Title: A Minimization Theorems for Verification Conditions
Author(s): Ward Douglas Maurer
E-Mail Address: maurer@ait.nrl.navy.mil
Citation: Proceedings of the 8th International Conference on Computing and Information Conference
Date: June 19-22, 1996
Report No.: AIT-96-012

Abstract

When using the inductive assertion method of proving the correctness of programs, there is some leeway as to how to choose the key points in the program at which the intermediate assertions are placed. Recent work in developing a verification condition generator (which produces the conditions necessary to prove a program correct) have had the surprising consequence that there really is one best way to choose key points, namely to choose exactly the joint points (that is, those with indegree greater than 1 in the directed graph of the program). We here justify this statement in several ways, the most important of which is that, if this method is chosen, the total internal size of verification conditions (that is, not counting the assertions at each end of a condition) is minimized, and the total condition size is very close to being minimized.

Title: A Scaleable Multicast Routing Algorithm For IP-ATM-IP Networks
Author(s): Mohammed Arozullah and Stephen G. Batsell
E-Mail Address: arozullah@pluto.ee.cua.edu
Citation: Proceedings of the 1996 IEEE Military Communications Conference
Date: 1996
Report No.: AIT-96-013

Abstract

Dynamic multicasting is needed in many military communication systems using IP-over-ATM networking. It is needed to provide multipoint-to-multipoint communication among members of multicast groups, many of which are both Senders and Receivers and join and leave the groups on dynamic basis. There may be many such multicast groups active at the same time. The situation is further complicated by the need to simultaneously establish, maintain, and tear down many point-to-multipoint SVCs with different QoS requirements on a dynamic basis in the ATM portion of the network. This requirement may prove to be difficult, time consuming, and in some cases impractical to satisfy. This may lead to unacceptably high delay and lack of scaleability.

This paper considers transmission of IP multicast packets over a large IP-ATM-IP communication network with the above mentioned characteristics and presents a multicast routing algorithm called Multipoint-to-Multipoint Routing Path With Branches (MMRPWB) algorithm for the ATM portion of this network. The algorithm presents, for each multicast group, steps for establishing a single multicast routing path that can be used by all sources (Senders) in this multicast group to multicast messages to all other group members simultaneously. Generation of the path starts at an arbitrary member node that sends a routing cell through the network. On receiving a copy of the cell, a node can decide to join the path if it is a member of the multicast group. Otherwise, it retransmits the cell forward. Details of the algorithm is presented in the body of the paper. The algorithm eliminates the need for establishment of individual point-to-multipoint routes for each Sender member of a multicast group and reduces overall number of SVCs required. The resulting multipoint-to-multipoint path uses only point-to-point SVCs and hence eliminates the problems associated with using point-to-multipoint SVCs. It also eliminates the need for dynamic IP to ATM address resolution. Performance of this multipoint-to-multipoint path has been shown to be superior to those of multicast routes established.

Title: Underwater Imaging with Acoustic Lens: Image Processing and Visualization
Author(s): Behzad Kamgar Parsi
E-Mail Address: behzad@ait.nrl.navy.mil
Citation: Naval Research Laboratory Formal Report, NRL/FR/5580--96-9826
Date: August 30, 1996
Report No.: AIT-96-014

Abstract

In this report, we discuss image processing, scene reconstruction, and visualization techniques used for underwater acoustic images taken with lens-based systems from a stationary platform. These systems are designed for high-resolution imaging of objects from distances of a few meters. The acoustic lenses used for beamforming in the imaging systems are made of crystal polystyrene, and are cut in cylindrical or spherical shapes. The cylindrical lens has a fan-shaped beam pattern and produces a 2D intensity image or shadowgram, while spherical lens with a cone-shaped beam produces a 3D intensity image. Test images obtained by the spherical lens contain a remarkable degree of detail.

Title: Relative Precision in the Inductive Assertion Method
Author(s): Ward Douglas Maurer
E-Mail Address: maurer@ait.nrl.navy.mil
Citation: Proceedings of the Workshop on Numerical Analysis and Applications
Date: June 24-27, 1996
Report No.: AIT-96-016

Abstract

The inductive assertion method of Floyd is here applied to programs involving floating point numbers, using a new verification condition generator for C programs known as ProveIt. The exit assertions of such programs need to state that the answers are correct to within some tolerance. We define this notion of tolerance, and show that it is equivalent to Olver's notion of relative precision. As an example, we present an $O(\iota\pi\ \pi)$ program which takes the πth power of a, and show that the speed of the program does not improve the relative precision, which remains 2π rather than the expected $2\ \iota\pi\ \pi$.

Title: The Use of Partial Functions in Proving That a Program Does Not Crash
Author(s): Ward Douglas Maurer
E-Mail Address: maurer@ait.nrl.navy.mil
Citation: Proceedings of the Workshop on Mechanization of Partial Functions
Date: July 30, 1996
Report No.: AIT-96-017

Abstract

The informal notion that "a program has crashed" is here rigorously defined to mean that it has attempted to execute some statement at a time when that statement is undefined. The statement is therefore a partial function, and proofs that programs do not crash must take account of partial functions. We show how this is done throughout the design of a newly constructed program correctness system.

Title: Localization in a Shallow Water Environment Using Inter-Array BroadBand Coorelation
Author(s): Wendell L. Anderson, Haw-Jye Shyu, and William R. Smith
E-Mail Address: wanderso@ait.nrl.navy.mil or shyu@ait.nrl.navy.mil or smith@ait.nrl.navy.mil
Citation: Naval Research Laboratory Formal Report, NRL/FR/5580--96-9828, publication of abstract, Document Classified, DIstribution Limited
Date: August 1996
Report No.: AIT-96-019

Abstract

This report examines acoustic inter-array broadband correlation processing for real-time tactical localization and tracking in a shallow water environment. Processing was performed using data recorded from three separate arrays as part of an at-sea test. Inter-array correlations produced detectable correlogram

traces of an underwater target from which consistent tracks could be computed. Simulation of the broadband propagation characteristics was used to estimate expected inter-array correlation parameter extraction errors and resulting localization uncertainties which are compared with using individual array beam crossing methods.

Title: Performance of Detect-On-Track in a High Shipping Environment
Author(s): Yung P. Lee and Haw-Jye Shyu
E-Mail Address: shyu@ait.nrl.navy.mil
Citation: Proceedings of the Ocean 96 MTS/IEEE-Prospects for the 21st Century, pp1313-1318
Date: September 23-26, 1996
Report No.: AIT-96-021

Abstract

A detect on-track algorithm based on the Hugh transform has been applied to acoustic broadband correlograms for passive detection and localization[1]. When normalized by the number of points, the Hough transform computes the arithmetic-mean along a track. The process is referred to as an arithmetic-sum (AS) transform. Two nonlinear transforms have been proposed: the logarithmic-sum (LS) transform and the harmonic-sum (HS) transform[2]. The LS-transform sums dB's, while the HS-transform sums the reciprocal of the power along the track. In this study, the detect-on-track algorithm has been modified and applied to the narrowband beamformed output. Several different beamforming approaches, including adaptive plane-wave beamforming and shaded plane-wave beamforming, were considered. The detect-on-track performance is evaluated against a typical scenario in a high shipping noise environment, using a dynamic simulation over a long time period.

Title: High-resolution Underwater Acoustic Imaging with Lens-based Systems
Author(s): Behzad Kamgar-Parsi, Bruce Johnson, Don Folds, and Ed Belcher
E-Mail Address: behzad@ait.nrl.navy.mil
Citation: International Journal of Imaging Systems and Technology (Special Issue)
Date: December 9-11, 1996
Report No.: AIT-96-022

Abstract

In recent years, several sonars designed for high-resolution, short range underwater imaging have been developed. These imaging systems use an acoustic lens to focus the incoming waves on an array of transducers. In this paper, we describe three prototype systems that use a line-focus or a point-focus lens, and operate at a frequency of 300 kHz or 3 Mhz. The line-focus lens produces 2D intensity images, while the point-focus lens produces 3D intensity

---

[1] "Application of the Hough Transform to Acoustic Broadband Correlogram for Passive Detection and Localization," Richard Stevens and Haw-Jye Shyu, NRL report NRL/MR/5580-92-7182.

[2] "Nonlinear Transformations for Spatial Matched-Filtering (Detect-On-Track)," Yung P. Lee (SAIC) and e Shyu (NRL), J. Acoust. Soc. Am., Vol. 97, No. 5, Pt. 2, pp. 3293, May 1995.

images. We present sample images taken from moving and stationary platforms, and discuss the techniques used for processing the acoustic backscatter data to reconstruct and visualize the scene. The images, particularly those taken with a point-focus lens, show a remarkable degree of detail.

Title: FinCen MPP
Author(s): Joseph B. Collins
E-Mail Address: collins@ait.nrl.navy.mil
Citation: FY 1995 NRL DOD High Performance Computing Modernization Program Annual Reports
Date: April 1996
Report No.: AIT-96-023

Abstract

The technical objective of this project is to investigate various analysis methods, applicable to categorical data, that require the use of high performance computing. These methods will be used to exploit the information in a large law enforcement database.

Title: Advanced Processor Technology
Author(s): Wendell Anderson, Becky Popp, Haw-Jye Shyu and William R.Smith
E-Mail Address: wanderso@ait.nrl.navy.mil or popp@ait.nrl.navy.mil or shyu@ait.nrl.navy.mil or smith@ait.nrl.navy.mil
Citation: FY 1995 NRL DOD High DOD High Performance Computing Modernization Program Annual Reports
Date: April 1996
Report No.: AIT-96-024

Abstract

Significance: Broadband correlation can be applied to the detection, localization, and tracking of both underwater and surface vessels by arrays of underwater sensors. This experience with the CM5E indicates that parallel high performance computer technology can provide both the large storage requirements and the large computational power required to perform this function in a real-time environment.

Title: Finite-Difference Time-Domain Simulations and Visualizations of Optical, Electromagnetic, and Acoustic Wave Propagation and Scattering in Complicated Environments
Author(s): James B. Cole and Neelam Gupta
E-Mail Address: cole@ait.nrl.navy.mil
Citation: FY 1995 NRL DOD High DOD High Performance Computing Modernization Program Annual Reports
Date: April 1996
Report No.: AIT-96-025

Abstract

We develop high-accuracy, high-performance parallel computer programs and algorithms to simulate the propagation and scattering of light and electromagnetic waves in complicated irregular structures, and complicated environments. Applications include Mie scattering, optical waveguide modeling, and radar scattering.

Title: Advanced Distributed Simulation
Author(s): Lawrence C. Schuette, Jeffrey M. Opper, William P. Niedringhaus, and Brian R. Winner
E-Mail Address: schuette@ait.nrl.navy.mil
Citation: FY 1995 NRL DOD High Performance Computing Modernization Program Annual Reports
Date: April 1996
Report No.: AIT-96-026

Abstract

Simulation is becoming an increasingly important component of the DOD technology base. In particular, Distributed Interactive Simulation (DIS) is being used more frequently to support simulated environments for training and concept evaluation. While DIS has demonstrated its utility in small scale applications, potential uses require scaling the technology to support substantially large scenarios involving 10,000 to 100,000 entitities. This research investigated strategies for using massively parallel processor to simulate large numbers of synthetic forces using a contemporary synthetic forces software systems.

Title: ALMDS Air Task
Author(s): Jerry L. Gorline
E-Mail Address: gorline@ait.nrl.navy.mil
Citation: FY 1995 NRL DOD High Performance Computing Modernization Program Annual Reports
Date: April 1996
Report No.: AIT-96-027

Abstract

The objective of this project is to develop a realistic model of a laser imaging system using high performance computing. Modeling of laser imaging systems is necessary to predict performance in various ocean environments. Two parameters that affect system performance include turbidity and sea state. The best technique for modeling time-dependent light propagation is with the Monte Carlo method.

Title: VR Goes Legit!
Author(s): Lawrence J. Rosenblum, Guest Editor
E-Mail Address: rosenblum@ait.nrl.navy.mil
Citation: IEEE Computer Graphics and Application
Date: 1996
Report No.: AIT-96-028

Abstract not available. Monthly column.

Title: Development of a Tactical Decision Aid for Shipboard Damage Control
Author(s): David L. Tate
E-Mail Address: tate@ait.nrl.navy.mil
Citation: Naval Research Laboratory Formal Report, NRL/FR/5580--96-9837
Date: November 20, 1996
Report No.: AIT-96-029

Abstract

Shipboard damage situations require rapid decision making to be performed to prevent serious injury to personnel, damage to ships systems, or loss of the ship. As the Navy proceeds toward more complex ships systems and reduced manning, a means of automating the decision making process is needed to assist damage control personnel in taking corrective actions. Because of the incompleteness or uncertainty of damage control information, conventional computational techniques are unsuitable for use in damage control situations. A tactical decision aid, based on expert systems technology, can be used to evaluate facts and their relative uncertainty, and apply a set of rules to draw inferences that lead to possible problem solutions.

This report describes the development of a tactical decision aid for shipboard damage control that uses a rule-based expert system based on information from Navy damage control tactics, procedures, and doctrine, together with information from fire research and firefighting experts. This expert system can receive information, assess its significance, and recommend corrective action. The expected payoffs include reduced damage control response time, consistency of responses and corrective actions, and a reduction in manning with no reduction in performance.

Title: Strike Visualization in Stereo on the Virtual Workbench
Author(s): Ranjeev Mittu and Jeffrey K. Uhlmann
E-Mail Address: mittu@ait.nrl.navy.mil or uhlmann@ait.nrl.navy.mil
Citation: Proceedings of the Worshop on Information Technology and Systems (WITS 96)
Date: December 14, 1996
Report No.: AIT-96-030

Abstract

The ability to view strike plans, such as routes for aircraft, radar detection envelopes, and terrain, is important to strike planners. A 3D view of the scenario provides the planner with an understanding of the important interactions and spatial relationships between the objects in the environment. Although current

strike mission planning/visualization systems provide an acceptable interface for viewing certain aspects of the strike environment, there are two areas that are deficient and need addressing in order to enhance mission planning and previewing. The first is the lack of a true 3D representation of the scenario. Current systems do work with 3D information, such as terrain, routes, etc. However, this 3D information is displayed on a monitor that is 2D. What is needed is a better approach to visualizing the important spatial relationships on a 2D monitor. The second item which is deficient is a poor visual representation of Radar Terrain Masking (RTM). The problem of representing RTM is of great importance to strike planners. When terrain obscures the view of a radar in a certain direction, we say that the terrain has masked the view of the radar. The ability to accurately identify RTM gives the planner a visual representation of where the "holes" are in the radars coverage. These ``holes" represent safe areas through which strike aircraft may avoid detection. Additionally, if the strike planner has to modify the routes, then the ability to visualize RTM is very important.

NRL has developed a Decision Support System (DSS), hereafter referred to as the Strike Optimized Mission Planning Module, or STOMPM. This decision aid serves as a testbed for research and development of asset routing algorithms, where the assets may be strike aircraft or missiles. These routing algorithms take into consideration the positions of enemy radars, intended targets, and the features of the terrain. We have investigated various techniques within this DSS which could improve current strike planning/visualization systems, particularly with regard to more realistic 3D displays and a better visual model for RTM.

Title: Shipboard VR: From Damage Control to Design

Author(s): Jim Durbin, Dan Fasulo, Upul Obeysekare, Lawrence J. Rosenblum, and David L. Tate

E-Mail Address: durbin@ait.nrl.navy.mil or tate@ait.nrl.navy.mil or rosenblum@ait.nrl.navy.mil

Citation: IEEE Computer Graphics and Applications

Date: November 1996

Report No.: AIT-96-031

Abstract

This article is an overview of two of the virtual reality projects currently under way in the Information Technology Division of the Naval Research Laboratory. The application domains described here are shipboard firefighting and simulation based design. The shipboard firefighting project developed and evaluated a virtual environment to verify the usefulness of VE for firefighter training and mission rehearsal under realistic conditions. The feasiblity tests performed aboard the ex-USS Shadwell showed that mission rehearsal in VE provided a measurable improvement in firefighter performance in terms of elapsed time and number of wrong turns. In the simulation based design project, the Responsive Workbench, a 3D tabletop projection system, was used to examine a preliminary design of the arsenal ship, a new ship design currently under development by the Navy. Using the 3D visualization and interaction techniques afforded by the Responsive Workbench, design errors and incosistencies were discovered earlier in the design process than they would have been using standard techniques.

1995 PUBLICATIONS

AIT-95-001 Reconstruction and Visualization of Underwater Objects from High-Resolution Acoustic Lens Data, *Behzad Kamgar-Parsi and Bruce J ohnson*

AIT-95-002 Finite-Difference Time-Domain Simulations of Wave Propagation and Scattering as a Research and Educational Tool, *J. B. Cole, R. A. Krutar, S. K. Numrich, and D. B. Creamer*

AIT-95-003 Technical Documentation of Nodestar, *Lawrence D. Stone, Thomas L. Corwin, and James B. Hofmann*

AIT-95-004 Distribution and Moments of The Weighted Sum of Uniform Random Variables, With Applications In Reducing Monte Carlo Simulations, *Behzad Kamgar-Parsi, Behrooz Kamgar-Parsi, and Menashe Brosh*

AIT-95-005 Autonomous Battle Damage Assessment Study, *Tamara Luzgin*

AIT-95-006 A High Accuracy FDTD Algorithm to Solve Microwave Propagation and Scattering Problems on a Coarse Grid, *James B. Cole*

AIT-95-007 Tactical BDA for Space and Electronic Warfare (abstract only), *Tamara Luzgin*

AIT-95-008 Threat Site Overflight Modeling for Strike Route Optimization, *Miguel R. Zuniga and Patrick Gorman*

AIT-95-009 Hyperbolic Pattern Detection Using the Hough and Fourier Transform, *Becky Popp*

AIT-95-010 Persistence in Computational Geometry, *Ali R. Boroujerdi*

AIT-95-012 Virtual Reality, Visualization and Their Application, *Rae E. Earnshaw and Lawrence J. Rosenblum*

AIT-95-013 Interactive Realism for Visualization Using Ray Tracing, *Robert A. Cross*

AIT-95-014 Infrastructure for Rapid Execution of Strike-Planning Systems, *James B. Hofmann, John Cleary, Darrin West, Larry Mellon, and Jim Ramsey*

AIT-95-015 Effectiveness of Various New Bandwidth Reduction Techniques in ModSAF, *Kevin L. Russo, Lawrence C. Schuette, Ph.D., Joshua E. Smith, and Matthew McGuire*

AIT-95-016 Network Routing Models Applied to Aircraft Routing Problems, *Zhiqiang Chen, Andrew T. Holle, Bernard M.E. Moret, Jared Saia, and Ali Boroujerdi*

AIT-95-017 High Accuracy Solution of Maxwell's Equations Using Non-Standard Finite Differences, *James B. Cole*

AIT-95-018 Coding and Compression with Flexible Transform, *Behzad Kamgar-Parsi, Behrooz Kamgar-Parsi, and Lawrence C. Schuette*

AIT-95-019 Virtual Reality: Research Issues and Applications, *Robert A. Cross and Lawrence J. Rosenblum*

AIT-95-020 Persistent Linked Structures at Constant Worst-Case Cast, *Ali R. Boroujerdi and Bernard M.E. Moret*

AIT-95-021 Estimating the Effective Depth of Laser Imaging Systems in Various Ocean Environments, *Jerry L. Gorline*

1994 PUBLICATIONS

AIT-94-001 Determinacy of Generalized Schema II, *Richard S. Stevens*

AIT-94-002 Time-Domain Visualization of Electromagnetic and Acoustic Wave Fields Computed with a Cellular Automaton Algorithm on a Parallel Computer, *James B. Cole, Rudolph A. Krutar and Susan K. Numrich*

AIT-94-003 Visualizing Noisy Underwater Acoustic Range Images, *Behzad Kamgar-Parsi and Behrooz Kamgar-Parsi*

AIT-94-004 A Prototype System for the Evaluation of Interdependent Routing Algorithms for Military Aircraft, *Ranjeev Mittu*

AIT-94-005 Advanced Technology for Precision Strike Planning, *James B. Hofmann and Dennis Carroll*

AIT-94-006 Weapon-Target Allocation for Force-Level Strike Planning, *Ray Jakobovits, Dennis Carroll Metron and James Hofmann*

AIT-94-007 High-Resolution Underwater Acoustic Imaging, *Behzad Kamgar-Parsi*

AIT-94-008 Progress and Problems in Ocean Visualization, *Lawrence J. Rosenblum and Behzad Kamgar-Parsi*

AIT-94-009 Challenges in the IV&V of C2E Software, *Dr. Kurt Askin, Kenneth W. Pitts, James E. Coolahan, et al.*

AIT-94-010 European Activities in Virtual Reality, Jose *Encarnacao, Matin Gobel and Lawrence Rosenblum*

AIT-94-011 Support Tools for the Processing Graph Method, *Roger Hillson*

AIT-94-012 Using the Hough Transform and the Fourier Transform to Detect Broadband Multipath Interference Patterns in Lofargram Images, *Becky Popp*

AIT-94-013 Cyberpower 2000: The Information Revolution, *Tamara Luzgin*

AIT-94-014 A Nearly Exact Second Order Finite-Difference Time-Domain Wave Propagation Algorithm on a Coarse Grid, *James B. Cole*

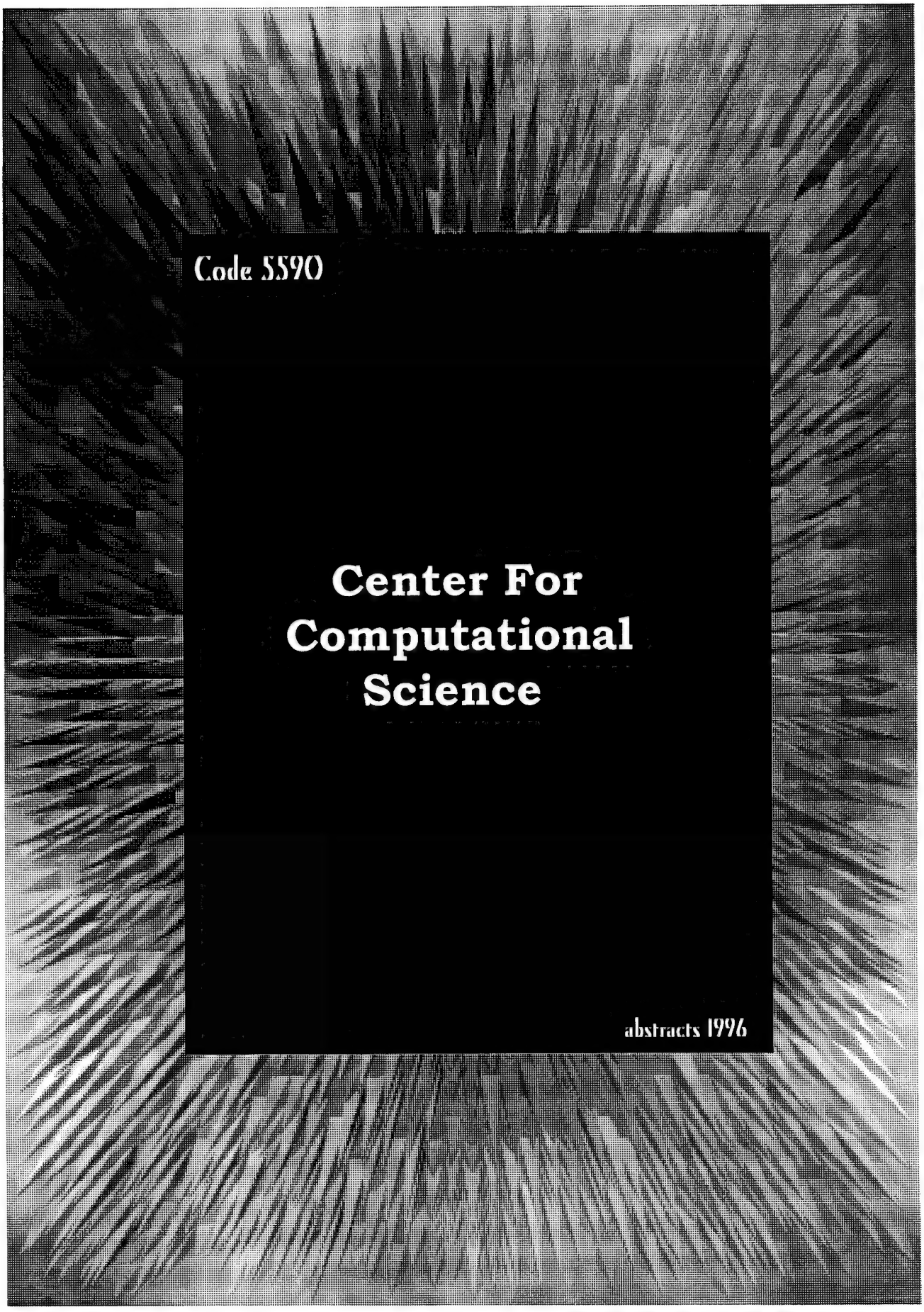
AIT-94-015 Data Consolidation and Connected Components, *Joseph B. Collins*

AIT-94-016 Observation on Operational Jointness, *Tamara Luzgin*

AIT-94-017 Research Issues in Scientific Visualization, *L. Rosenblum, Guest Editor*

AIT-94-018 Research Issues in Volume Visualization, *Arie Kaufman, Karl Heinz Hohne, Wolfgang Kruger, et al.*

AIT-94-019 Visualization Blackboard Department, *L. J. Rosenblum, Editor*


Code 5590
Center For
Computational
Science
abstracts 1996

CENTER FOR COMPUTATIONAL SCIENCE

CODE 5590

The Center for Computational Science (CCS), Code 5590, conducts research and development to further the advancement of computing and communications systems to solve Navy problems. The Branch accomplishes this mission through a balanced focus on service, research, and development. The Center is committed to investigating and developing leading edge technologies to establish an advanced computational environment that will benefit all research areas. The Branch studies new technologies to evaluate their potential. Promising technologies are further developed, enhanced, and transitioned to production systems. The Branch's operational efforts provide for a computing environment that emphasizes reliability, high performance, and user productivity. In the area of research and development the Branch develops and implements new technologies, both hardware and software, to solve Navy problems in diverse application areas. Current thrusts include: parallel and distributed hardware, software and display technologies; signal processing techniques directed toward exploitation of massively parallel systems; development of hardware architecture independent systems for developing and porting code for parallel processing; and development of high-speed networks.

In the area of operational support, the Center provides shared high performance computing and networking resources and related services, including user support and training, for NRL, Navy, and DoD interdisciplinary research efforts. The Branch manages and operates NRL's shared massively parallel supercomputer, vector mini-supercomputer, central file server/archiver, and scientific visualization systems. The Branch has responsibility for the laboratory's local area network and external connections to network and computer systems world-wide. The Branch also provides laboratory ADP logistic support by identifying ADP requirements and securing and administering contractual support for lab-wide or multiple buys of ADP systems, software and services.

Title: FY95 NRLDoD High Performance Computing Modernization Program Annual Reports
Author(s): Jean Osburn
E-mail Address: osburn@bohr.nrl.navy.mil
Citation: NRL/PU/5590--96-0001
Date: Feb. 13, 1996
Report No.: CCS-96-001

Abstract

These reports summarize the accomplishments of the NRL Principal Investigators who received computer allocations on the DoD High Performance Computing Modernization Program Shared Resource Centers in FY95

Title: Visualizing Time-Dependent Particle Traces in the Context of Real-Time Visualization Environment
Author(s): Upul R. Obeysekare, Fernando Grinstein, and Gopal Patnaik
E-mail Address: grinstei@lcp.nrl.navy.mil or patnaik@lcp.nrl.navy.mil
Citation: IEEE VISUALIZATION '96 Conference Proceedings, Hyatt Regency, San Francisco Airport, San Francisco, CA
Date: Oct. 27 - Nov. 1, 1996
Report No.: CCS-96-002

Abstract

Real-time visualization (RTV) is a process where visualization is performed on a local graphics workstation while the computationally intensive part of the simulation is performed either locally or remotely on a high performance workstation or supercomputer. This paper describes issues involved in generating time-dependent particle traces in the RTV environment. The technique proposed in this paper uses visual programming environment across heterogeneous computer architectures to create a flexible environment for visualizing particle trajectories released in a flow field. A numerically simulated non-circular jet is used to evaluate the use of the technique. Particle velocities at each time step are calculated based on local tri-linear interpolations of the instantaneous flow field data; particles are displayed as spheres that can be optionally colored using other scalar variables in the flow field. At any time of the simulation, the modular implementation of the method allows users to clear trajectories or start new ones at chosen seed points.

Title: Virtual Workbench - A Non-Immersive Virtual Environment for Visualizing and Interacting with 3D Objects for Scientific Visualization
Author(s): Upul R. Obeysekare, Charles J. Williams, Jim Durbin, Larry Rosenblum, Robert Rosenberg, Fernando Grinstein, Ravi Rammamurti, Alexandra Landsberg, and William Sandberg
E-mail Address: grinstei@lcp.nrl.navy.mil
Citation: IEEE VISUALIZATION '96 Conference Proceedings, Hyatt Regency, San Francisco Airport, San Francisco, CA
Date: Oct. 27 - Nov. 1, 1996
Report No.: CCS-96-003

Abstract

The Virtual Workbench (VW) is a non-immersive virtual environment that allows users to view and interact with stereoscopic objects displayed on a workspace similar to a tabletop workspace used in day-to-day life. The nature of its design enables the VW to simulate the viewing volume of the viewers to be partially below and above the tabletop surface. This feature can be exploited to create views that correspond to real environments. VW is also an ideal environment for collaborative work where several colleagues can gather around the table to study 3D virtual objects.

Initial implementation of this device [1], (reported as Responsive Workbench) was primarily for medical applications, virtual architecture designs and for a few scientific visualization cases. Virtual Reality laboratory at the Naval Research Laboratory has implemented the VW using a concept similar to what is reported in [1]. This paper investigates how the VW can be used as a non-immersive display device for understanding and interpreting complex objects encountered in the scientific visualization field. Different techniques for interacting with 3D visualization objects on the table and using VW as a display device for visualization are evaluated using several cases.

Title: Article for the DOD High Performance Computing Modernization Plan Requirements Survey Team
Author(s): Jean E. Osburn
E-mail Address: osburn@bohr.nrl.navy.mil
Citation: HPCMP Requirements Survey Team
Date: April , 1996
Report No.: CCS-96-004

Abstract

This is an article written for the DOD High Performance Computing Modernization Plan (HPCMP) Requirements Survey Team. This was written upon their request of Naval Research Laboratory's Service/Agency Approval Authorities, Codes 5594 and 7034. The requirements teach is assembling a document to circulate both inside and outside DOD. The intent is to capture an accurate description of our agency's mission, its vision of HPC, and a summary of its HPC requirements.

Title: Real-Time Visualization of Numerically Simulated Jet Flows Using NASA/NAS'S Live
Author(s): Upul R. Obeysekare, Fernando Grinstein, and Gopal Patnaik
E-mail Address: grinstei@lcp.nrl.navy.mil or patnaik@lcp.nrl.navy.mil
Citation: The NAS Systems of NASA Ames Res Ctr, Mountain View, CA.
Date: 1996
Report No.: CCS-96-005

Abstract

The NAS systems of NASA Ames Research Center in Mountain View, California has implemented a visualization system called Large-Scale Interactive

Visualization System (LIVE) for those visualization tasks that require resource intensive visualization techniques or interactive visualization methods. The LIVE system consist of a large visualization computer with a lot of memory, high speed disks, access to supercomputers via high-speed networks, and software to support large visualization tasks. This report provides results and analysis for an exercise using the LIVE systems for Real-Time Visualization (RTV) of numerically simulated jets.

RTV is a process where visualization is performed on a local graphics workstation, while the computationally intensive part of the simulation is performed either locally or remotely on a high performance workstation or a supercomputer. The RTV technique implemented for this study used the NAS Cray C90 supercomputer and Silicon Graphics Power Onyx system connected via HIPPI network to visualize flow solvers, using the Application Visualization System (AVS) software. Relevant issues and difficulties involved in this implementation of RTV, with emphasis on interactive control of numerical simulations, are being described. Important issues governing the implementation of this technique, such as network data transfer speeds, asynchronous module execution, architecture neutral implementations, visual programming environment across heterogeneous computer architectures, and user-interface design for visual control of the simulation, are being presented. Finally, the results from using the LIVE system are been analyzed in the context of selected numerical simulations.

Title: Visualizing Time-Dependent Particle Traces in the Context of Real-Time Visualization Environment
Author: Upul R. Obeysekare, Fernando Grinstein, and Gopal Patnaik
E-mail Address: grinstei@lcp.nrl.navy.mil or patnaik@lcp.nrl.navy.mil
Citation: 35th AIAA Aerospace Sciences Meeting and Exhibit, Reno, NV
Date: Jan. 6-9, 1997
Report No.: CCS-96-006 (Resubmission of CCS-96-002)

Abstract

Real-time visualization (RTV) is a process where visualization is performed on a local graphics workstation while the computationally intensive part of the simulation is performed either locally or remotely on a high performance workstation or supercomputer. This paper describes issues involved in generating time-dependent particle traces in the RTV environment. The technique proposed in this paper uses visual programming environment across heterogeneous computer architectures to create a flexible environment for visualizing particle trajectories released in a flow field. A numerically simulated non-circular jet is used to evaluate the use of the technique. Particle velocities at each time step are calculated based on local tri-linear interpolations of the instantaneous flow field data; particles are displayed as spheres that can be optionally colored using other scalar variables in the flow field. At any time of the simulation, the modular implementation of the method allows users to clear trajectories or start new ones at chosen seed points.

Title: Interactive Desktop Laboratory With Visual Supercomputing
Author(s): Upul Obeysekare, Fernando Grinstein, and Gopal Patnaik
E-mail Address: grinstein@LCP.nrl.navy.mil or patnaik@LCP.nrl.navy.mil
Citation: IEEE Computational Science and Engineering Visual Supercomputing, Los Alamitos, CA
Date: Sept. 1, 1996
Report No.: CCS-96-007

Abstract

We discuss practical implementation aspects of the Interactive Desktop Laboratory (IDL), consisting of a fully functional virtual laboratory on the desktop computer. In the IDL framework, the results of large-scale numerical simulations performed on (generally-remote) supercomputers are displayed visually in real-time on the screen of a local workstation. Simulation steering is performed interactively by modifying control parameters on the user interface, based on direct feedback provided by the visualizations as the computer experiments are in progress. An attractive feature of our approach is to implement the IDL concept in a general and flexible environment as opposed to one that is subject or hardware specific.

The IDL concept offers a useful environment for conducting numerical experiments on the desktop, where distributed and modular implementation can be fully exploited to select optimal architectures and diagnostics to efficiently match the problem under study. In addition, replacing the desktop console with virtual environments can considerably improve the model interpretation process. Results of ID implementations in case studies involving jet simulations are presented.

Title: A 4096 Atom Model of Amorphous Silicon: Structure and Dynamics
Author(s): Brian Davidson, Joseph L. Feldman, Scott R. Bickham, and Frederick Wooten
E-mail Address: davidson@volt
Citation: NRL/OP/5590--96-0008
Date: March '97 Meeting of the American Physical Society in Kansas City, Mo.
Report No: CCS-96-008

Abstract

We present structural and lattice dynamical information for a 4096 atom model of amorphous silicon. The structural model was obtained, similarly to previously published smaller models, using periodic boundary conditions, the Wooten-Winer-Weaire bond-switching algorithm, and the Broughton-Li relaxation with respect to the Stillinger-Weber potential. The structure is dynamically stable, and there is no evidence in the radial distribution function of medium range order. For examining this large model, we use a 1000 processor Connection Machine to compute all the eigenvalues and eigenvectors exactly. The phonon density of states and inverse participation ration are compared with results for related 216, 432 and 1000-atom models

---

1995 PUBLICATIONS

CCS-95-001 An Application for Visualizing Molecular Dynamics Data Developed Under AVS/Express, *Upul R. Obeysekare and Chas J. Williams*

CCS-95-002 CM-5 Kernel Optimization of a Global Weather Model, *P.B. Anderson, D.W. Norton, and M.A. Young*

1994 PUBLICATIONS

CCS-94-001 On Commonalities In Signal Design for Non-Gaussian Channels, *Nhi-Anh Chu*

CCS-94-002 Visualizing Time Dependent Data From Molecular Dynamics Simulations Using AVS, *Upul R. Obeysekare, Chas J. Williams and Robert O. Rosenberg*

CCS-94-003 Real-Time Visual Control of Numerical Simulations, *U.R. Obeysekare, F.F. Grinstein, Chas J. Williams, and G. Patnaik*

CCS-94-004 Connection Machine Software Conversion of the Navy TOPS Model, *Paul B. Anderson and Michael A.Young*